

History of malware

Nikola Milošević

inspiratron.org

Abstract

In past three decades almost everything has changed in the field of malware and malware analysis. From malware created as proof of some security concept and malware created for financial gain to malware created to sabotage infrastructure. In this work we will focus on history and evolution of malware and describe most important malwares.

1. Introduction

Malware, short for **malicious** (or malevolent) **software**, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses [1].

History of malware can be split to several categories that will also represent timeframe in which events from that category happened. So we will split history of malware in 5 categories. First category is early phase of malware. This is time when first malwares come to life. Second phase is early Windows phase. It will describe first Windows malwares, first mail worms and macro worms. Third part is evolution of network worms. These threats become popular when internet becomes wide spread.

Forth part is rootkits and ransomwares. These were the most dangerous malware before 2010. Then came malware that was made for virtual espionage and sabotage. This malwares were created by secret services of some countries. This is the last phase of malware evolution that we are now facing.

In this work we will describe malware evolution in these five phases. Also in this work we will not describe all malware, but just malware that were great game changers, and was most famous by introduced new things in malware world.

2. Beginnings of malware

There were some malware for other platforms before 1986., but in 1986. appeared first malware for PC. It was virus called Brain.A. Brain.A was developed in Pakistan, by two brothers - Basit and Amjad. They wanted to prove that PC is not secure platform, so they created virus that was replicating using floppy disks. It infected booting sector of floppy drive and booting sector of every inserted floppy disk. So anytime infected floppy would be inserted into PC, it would infect it's drive, so the drive would infected again every disk inserted.

This virus did no harm, and authors were signed in code, with phone numbers and address [2]. Intention of early malware writers was to point on problems, rather than make some harm or damage. But later of course malware become more and more destructive.

After Brain there were other viruses. One of the interesting is **Omega** virus. It was called Omega because of omega sign that it was writing in some conditions in console. It was infecting boot sector, but was not doing much damage unless it was Friday 13th. On that day PC could not boot.

Michelangelo virus would on Michelangelo's birthday in year 1992 rewrite first 100 sectors of hard disk[3]. Doing this, file allocation table would be destroyed and PC could not boot. **V-sign** is virus that also infected boot sector and wrote V sign on screen every month.

Walker is next virus that was quite visual and appeared in 1992. It was animating walker walking from one side of screen to the other. **Ambulance** virus was quite similar to Walker, animating ambulance car driving from one side of screen to the other, but it also added sound effects of ambulance car. One of the most interesting virus from the beginning of 1990' was **Casino virus**.

Casino virus would copy file allocation table to memory and delete original file allocation table. Then he will offer a slot game to user. User had to get 3 £ signs if he wants to use his PC and user could try three times. If user restarts machine the file allocation table would be gone, and machine would not be able to boot. Same would happen if user loses - file allocation table would be deleted from memory as well. If user wins the game, virus would copy back file allocation table from memory, and PC could be used normally.

Next big step in malware evolution was introduction of **mutation engine (MtE)**. Mutation Engine was created by Bulgarian hacker who called himself Dark Avenger. It was tool that could add mutation functionality to viruses, so they would be harder detected by anti-viruses. Basically this was first polymorphism module that could take any virus and make it far more invisible. Until mutation engine anti-virus software were finding viruses on PCs using file signatures and changes in file signatures. Introduction of polymorphism made this method ineffective[5].

Virus creation laboratory was first UI tool for creating viruses. User could select features of virus and create it. This made virus creation easy. It has some disadvantages, but almost anyone using this GUI tool could create virus[6].

3. First windows malwares

When Windows was released it was interesting for many users since it gives powerful user interface. That simplicity of use attracted many users. Everything that has many users in computing world soon becomes interesting also for attackers and malware creators.

WinVir was first Microsoft Windows virus. It was also not doing much harm, it's main feature was that it was replicating, and that it was first virus that has ability to infect windows PE (Portable Executable) files. WinVir was doing little changes to infected files. When infected file was executed, WinVir was looking for other PE files and was infecting them. While WinVir was infecting other files original executed was rolled back to it's original state. To say it simple WinVir was deleting itself.

Monkey was virus that was infecting master boot record of hard drives and floppies. Monkey was moving first block of master boot record to third and inserting it's own code into first block. When infected computer was booted it was running normally, unless it was booted from floppy. In this case "Invalid drive specification" message was printed.

One-half or Slovak bomber was one interesting and might be quite destructive virus. It infected master boot record, EXE and COM files, but did not infected files that in name contained words like SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, MSAV or CHKDSK. These files were not infected because they might belong to some antivirus software, so the virus might be caught by auto-checking algorithms. It was encrypting parts of users hard drive using XOR function with some key known to virus. But if user tries to access some encrypted file, file was decrypted and user wouldn't notice anything. The problem with this virus was, that if it was cleared inappropriately, encrypted files couldn't be retrieved anymore[7]. Virus was showing message every 4th, 8th, 10th, 14th, 18th, 20th, 24th, 28th and 30th every month under particular circumstances:

Dis is one half.

Press any key to continue ...

Concept (WM.Concept) was first macro virus and it was detected in 1995. It was written in Microsoft Word macro language, and it was spreading by sharing documents. It worked on PC computers and on Macintosh computers if on computer was installed Microsoft Word. When document infected with Concept was opened on some PC, virus would copy it's malicious template over

master template, so every new document created on that computer would be infected[8].

Laroux (X97M/Laroux) was first Microsoft Excel macro virus. It was written in Visual Basic for Application (VBA), macro language for Office documents that was based on Visual Basic. It worked on Excel 5.x and Excel 7.x. It also could be run on Windows 3.x, Windows 95 and Windows NT. It was not making any harm, it was just replicating.

Boza was first virus that was written specifically for Windows 95. It was infecting Portable EXE files - files that were using Windows 95 and Windows NT. But it was not attacking Windows NT. So far, there was no virus detected that was written particularly for Windows NT. Virus was detected on January 1996. It had Australian origins, but it was detected all over the world. When file infected with Boza would be run, it would infect other files in that directory. One to three files would be infected on each run. After this Boza would run original program. Virus would not be active in memory anymore.



Boza virus message window

Boza was spreading quite slow, but also the spreading algorithm was fast enough that it could not be detected by user. Boza had no destructive routines, but it has one error that caused that under some circumstances infected files could

raise to several megabytes. This was problem on machines which hard disks were just few tens on megabytes large. Virus had activation routine that showed message window on every 31st of any month. Messages were: "The taste of fame just got tastier!" and "From the old school to the new".

Marburg (Win95/Marburg) is virus that started to circulate in August 1998., when it has infected master CD of MGM/EA PC game called Wargames. Publisher MGM on 12th of August 1998. released apologies to users:

*From: "K.Egan (MGM)"
<kegan@mgm.com>
Subject: MGM WarGames Statement
Date: Wed, 12 Aug 1998 18:03:39 -0700*

MGM Interactive recently learned that its WarGames PC game shipped with the Win32/Marburg.a virus contained in the electronic registration program. The company is working as fast as it can to resolve the problem ... MGM Interactive is committed to delivering top quality products to consumers. This is an unfortunate circumstance and we sincerely apologize for any convenience this has caused you. ... If you have any questions or if you would like to receive a replacement disc, please contact MGM Interactive.

Same virus was on CD that covered Austrian PC magazine Power Play in August 1998.

Maburg is polymorphic virus that infected Win32 and SCR (screen saver) files and encrypted it's code with polymorphic variable layer of encryption. Polymorphic engine of virus was quite advanced since it was encrypting virus with 8,16 and 32 bit keys and several different methods. Virus was using slow polymorphism, which means that it was changing it's

decryptor slowly. Maburg was deleting integrity database of several antivirus programmes. Also it was avoiding infecting files that was belonging to antivirus software and it was not infecting files containing V in name. This was done to prevent auto checking of antivirus software. Maburg was activated 3 months after infection if infected file was run at same hour as hour of infection showing standard MS Windows error icon (white cross in red circle) all over the desktop[9].



Maburg

Happy99 is first mail virus. It was spreading as attachment of e-mail as executable and was detected in 1998. At that time spam filters barely existed, and was allowing sending of executables. If user clicked and run the attachment, it would show him screen with fireworks, but also virus would replicate attachment and send mail to all user's contacts.

Melissa was virus that combined techniques of macro virus and mail virus. It was coming with attached infected MS Word file. If file was opened it would replicate to randomly chosen document from user's hard disk and send it to all contacts. This was quite problematic because of information leakage. Also virus was sometimes adding quotes from The Simpsons to infected documents[3].

LoveLetter was one of most successful social engineering virus. It was using premises of love, attracting user to open attachment. Attachment file would run

the virus. Virus was rewriting some quite important files on victim's system. Using premises of love virus convicted millions to open attachment, what caused financial damage of 5,5 billion dollars over the world. **Anakurnikova** was similar virus that was sending executable file, and convicting victims that there are sexy photos of Ana Kurnikova, sexy tennis player. Many was convinced to open file, and even when antivirus companies made detection and blocking of running malicious attachment, many asked support of companies, how they can see the pictures.

Worms

At the end of 1980's accidentally was created first PC worm. In 1988. Robert Tappan Morris, who was at that time student of MIT wrote a program that will be big game change event in malware history. As part of his project Morris wanted to count computers connected to internet. So he wrote little program that would replicate from one connected computer to another and count. But Morris made a bug, the worm was also visiting computers that it has already visited before. Actually worm was replicating from infected computer to all other connected computers all the time. This generated a lot of network traffic and almost crushed internet of that time. Because of this mistake Morris was arrested and convicted by Computer Fraud and Abuse Act from 1986[10]. This was also first case that someone was convicted by this law. At that time computers had open ports and connections and replications could be done without use of exploits. In the beginning of internet no one really thought about internet security. This made easy for Morris to make his worm.

But later security mechanisms was implemented and later worms had to use exploits to gain access to computer on network.

Internet worms work in way that they have scanning algorithm that scans network. In most cases it tries public or both public and private IP addresses. IP address could be unassigned, or it can be assigned to device that could not be attacked (wrong platform) or patched and protected computer. In this cases worm would not attack. But if computer on IP address is running on right unpatched platform, worm would use exploit to gain access to that computer. After that it would add some payload, that could trigger on some time or do some bad things to system. Then it would again start scanning network and try to propagate from that computer.

Code Red is first internet worm that came after Morris worm and that did not needed any user interaction. Also Code Red is first intentionally written worm (Morris worm was malicious by accident). Code Red was spreading in year 2000., and spread over the world in couple of hours. It was successfully hiding from defending mechanisms and had several capabilities that was triggered in cycles. It was attacking IIS (Internet Information service) web servers. First 19 days it only spread over the network using vulnerability in IIS. From day 20 do day 27 it lunched denial of service attacks on couple of websites (ie. Whitehouse). Last 3-4 days of month it would just rest.

Nimda was discovered on September 18th 2001.. Nimda fast spread over the world as internet worm. If Nimda letters switch position it would be admiN. Nimda was quite similar to Code Red by scanning network and propagating, but it had additional features. Scanning

algorithm of Nimda was scanning all IP addresses while Code Red was scanning just public IP range. Because of this feature Nimda could go further infecting private networks[3]. Nimda also had ability to change hosted website, so they would offer download of infected files. This way spreading of Nimda was even faster and more dangerous, because with user interaction Nimda could overcome firewalls and spread from that private computer hosts. It could spread to Windows 95,98, Me, NT 4 and Windows 2000. Nimda had one error because of which it was under some circumstances crushing and could not spread more.

Fizzer is mail worm from 2003. This was not internet worm, but we will describe it here, because of timeframe when it was found. Fizzer was first malware which only purpose was to generate revenue and money. It came in infected attachment, and was turning infected machine in spam sender.

In this period changes the structure of malware writers. Before Fuzzer, malware was written by enthusiasts that would like to proof something or to show up. From Fuzzer main focus on malware writers is gaining profit. After Fuzzer many malware come that sent spam or that blackmailed computer users. Also malware writers were not mostly from developed countries like it was in 1980' and 1990'. Main sources of malware came on 2000' by people from third world countries, mainly Russia, China, Pakistan, India etc.

Slammer was found on September 13th 2003., and brought some new things. It was internet worm that used vulnerability in OpenSSL and it is one of first malwares that attacked Linux machines and Apache servers. It also had a backdoor, so attacker could use

infected machine, upload to it some additional tools or malwares. Backdoor was creating UDP socket with attacker. Actually it was listening on UDP port 2002 for attacker's connection.

In years 2003 and 2004 was discovered 3 most destructive internet worms that have introduced consideration in security of real systems (factories, power plants, airports and other transportation systems) and virtual sabotage.

Slammer was internet worm that was spreading in 2003. using vulnerability in Microsoft SQL Server and Microsoft Data Engine 2000. Every application that used some of these two services was potential target and entrance point for Slammer. Some of applications that Slammer used to gain access to system were:

- Microsoft Biztalk Server
- Microsoft Office XP Developer Edition
- Microsoft Project
- Microsoft SharePoint Portal Server
- Microsoft Visio 2000
- Microsoft Visual FoxPro
- Microsoft Visual Studio.NET
- Microsoft .NET Framework SDK
- Compaq Insight Manager
- Crystal Reports Enterprise
- Dell OpenManage
- HP Openview Internet Services Monitor
- McAfee Centralized Virus Admin
- McAfee Epolicy Orchestrator
- Trend Micro Damage Cleanup Server
- Websense Reporter
- Veritas Backup Exec
- WebBoard Conferencing Server[11]

Slammer was spreading as an memory process. It never wrote anything on hard disk. So when PC would be restarted, infection would disappear. But since PC was connected to other PCs, from where it got infection, or where it replicated infection to, soon infection would be back. Slammer was creating great network traffic, so many packages become lost. This way it caused great damage - for example ATM network of Bank of America was down, 911 service in Seattle was down for couple of days, flight control systems on couple of airports were infected and some flight were delayed. Also there was a problem in nuclear power plant in Ohio.

Blaster was detected in August 2003. It used buffer overflow vulnerability in DCOM RPC (Distributed Component Object Model Remote Procedure Call). Blaster was used to create SYN flood to windowsupdate.com website, but since it was wrong website, real one was windowsupdate.microsoft.com, it did not caused much damage to Microsoft. But since it created traffic it did slow down and disable several systems like Air Canada planes were landed, US train company CSX stopped etc.

Sasser in 2004 used buffer overflow in Local Security Authority Subsistem Servis (LSAS). It spread over the network and it was quite often crashing LSAS service, which caused restart in one minute. When Microsoft released patch it was quite large to download and install in less time than time malware needed to crush LSAS service. This caused a lot of frustration for users, so soon new model of automatic updates was developed. Sasser caused Railcop trains to stop in Australia, Delta airlines problem and delays on British Airways flights, Hong Kong government department of energy was infected, two

hospitals in Sweden was infected and could not run scanners, EU commission was infected, Heathrow airport had problems with this malware, as well as UK Coastguard and several Banks closed their offices for couple of days because of internal infection.

5. Rootkits and ransomware

RootKits are malware tools that modify existing operating system software so that an attacker can keep access to and hide on a machine. RootKits can operate at two different levels, depending on which software they replace or alter on the target system. They could alter existing binary executables or libraries on the system. In other words, a RootKit could alter the very programs that users and administrators run (for example ls, cd, ps or other programs). We'll call such tools user-mode RootKits because they manipulate these user-level operating system elements. Alternatively, a RootKit could go for the jugular, or in our case, the centerpiece of the operating system, the kernel itself. We'll call that type of RootKit a kernel-mode RootKit [3].

First RootKit ever made was made by SONY Entertainment, and had quite bad impact on SONY's reputation. **SONY BMG RootKit** was born in year 2005, as idea of SONY to protect copyright of their publications. They had idea to detect and disable coping of their publications using this RootKit to other media. Sony BMG RootKit was part of 52 publications of Sony amongst them albums by Ricky Martin and Kelly Minogue. When CD was inserted in normal CD player or discman nothing would happen. But when CD was inserted in PC, RootKit would be installed, hide itself and all files starting with \$sys\$. Also it would control how

user accesses music. If user tries to copy RootKit would prevent it. Functionality to hide all files starting with \$sys\$ used other malware writers to hide their files on system calling malware files with starting \$sys\$. When RootKit was detected, there was great scandal because Thomas Hesse, Director of global sales in Sony BMG made statement in which he said "Most people, I think, don't even know what a rootkit is, so why should they care about it?". This caused heavy public reaction and had bad impact on SONY image. This is also shown as good example of bad public relations. There was also a law suit which epilogue was that SONY offered customers refund and free music downloads from website.

StormWorm was mail worm that came 7 years after LoveLetter, and same as LoveLetter used social engineering to spread. It used fear and horror instead of love, as LoveLetter did. StormWorm start spreading using mail with subject "230 dead as storm batters Europe". Also there was other manifestations as time passes, so some of the subjects of StromWorm were:

- A killer at 11, he's free at 21 and kill again!
- U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel
- British Muslims Genocide
- Naked teens attack home director.
- 230 dead as storm batters Europe.
- Re: Your text
- Radical Muslim drinking enemies's blood.

- Chinese/Russian missile shot down Russian/Chinese satellite/aircraft
- Saddam Husain safe and sound!
- Saddam Hussein alive!
- Venezuelan leader: "Let's the War beginning".
- Fidel Castro dead.
- If I Knew
- FBI vs. Facebook

Infected machines were creating a botnet network. But, since most botnet networks are controlled by one central server, this was not case with StormWorm, which was acting more like peer-to-peer network, so controlling node could change from host to host. StormWorm was installing also RootKit which it used to hide itself. Later variants, starting around July 2007, loaded the rootkit component by patching existing Windows drivers such as tcpip.sys and cdrom.sys with a stub of code that loads the rootkit driver module without requiring it to have an entry in the Windows driver list.

Mebroot from 2008 brought one new thing that changed the game - victim could be infected just by surfing internet from browser. It used exploit in browser to gain access to system, and one of the first websites used to spread this malware was official website of Monica Belluci. When Mebroot gained access to victims PC it would install rootkit that could hide him from RootKit detectors, which become part of many antivirus solutions. Mebroot was spying what victim was typing and it was sending this data to attacker. Also this malware was quite good debugged, so it almost never caused crashes of system. Even if it caused crash, it could collect and send traces to attacker so he can debug and fix

the problem. Doing this it was the most advanced malware at that time.

Conficker is one of the greatest mysteries in malware history. The intention of malware creator was not found. It used vulnerability in windows and cracking weak passwords for spreading. It would install backdoor, rootkit and created a botnet node on infect machine. It had infected about 10 millions of host. Great mystery is that it had very complex botnet network that was never used for any attack.

Interesting ransomware is malware that had encrypted victims hard disk, changed desktop background with message and demanded 120\$ for decryption key. Interesting thing was that attackers were giving away keys if they were paid. For spreading it used browser vulnerability and infected PDF files with script that downloads and installs this malware. It would change desktop background and place on desktop how-to-decrypt.txt file in which was this text:

Attention!!!

All your personal files (photo, documents, texts, databases, certificates, kwm-files, video) have been encrypted by a very strong cypher RSA-1024. The original files are deleted. You can check this by yourself - just look for files in all folders.

There is no possibility to decrypt these files without a special decrypt program! Nobody can help you - even don't try to find another method or tell anybody. Also after n days all encrypted files will be completely deleted and you will have no chance to get it back.

We can help to solve this task for 120\$ via wire transfer (bank

transfer SWIFT/IBAN). And remember: any harmful or bad words to our side will be a reason for ingoring your message and nothing will be done.

For details you have to send your request on this e-mail (attach to message a full serial key shown below in this 'how to..' file on desktop): [email address]

Files that were crypted on disk had extensions: .jpg, .jpeg, .psd, .cdr, .dwg, .max, .mov, .m2v, .3gp, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .rar, .zip, .mdb, .mp3, .cer, .p12, .pfx, .kwm, .pwm, .txt, .pdf, .avi, .flv, .lnk, .bmp, .1cd, .md, .mdf, .dbf, .mdb, .odt, .vob, .ifo, .mpeg, .mpg, .doc, .docx, .xls, and .xlsx..

6. Virtual sabotage and espionage

In year 2010., one big step in malware evolution happened. Malware is no more seen just like threat for businesses, personal finances or files. Military, police forces and secret agencies of several countries got involved in malware creation. Malware is now seen similar as any other weapon. US government declared that any US army keeps right to respond to cyber attack with physical attack. Dropping bombs and cyber attacks using malware are seen as equal things. Also, malware become capable of doing almost same damage as bomb, but without risking human lives. The best example for that is malware called **Stuxnet**, which was discovered in summer 2010.

Stuxnet is a first so called super malware, found in June 2010., but when it was found it is realized that it was spreading undetected for about a year. When Stuxnet was detected it has

already done what it was built for. It is believed that Stuxnet was created to destroy or at least slower down Iranian nuclear program. Stuxnet physically sabotaged turbines for uranium enrichment by changing rotation frequencies. This was done in way that was not seen before. Stuxnet was spreading over the USB stick, where turned off auto run or auto play option would not help. If USB stick was inserted in infected PC it would be infected and if infected USB was inserted in PC, PC would be infected. No anti-virus was able to detect it. Stuxnet used rootkit to hide itself on infected machine and it would do nothing else but replicating to other inserted USB sticks. For gaining control over the PC it used 5 exploits from which 4 was on the day when Stuxnet was first detected 0-day exploits. It would activate it's routines just in case it PC was attached to particular Siemens Step 7 controller, and the PC would be used for programming of controller. Even in that case it would not do anything, if the controller is not attached to particular industrial system. In that case it would changes frequencies of rotation system, and it would also reprogram tools for automatic response, so it would look for them as the system works correctly. Stuxnet contained valid certificate, and when it was blacklisted in one day period it changed its certificate. It had death date set on June 24th 2012., when all instances of Stuxnet would kill itself. It is believed that this malware was created by secret services of USA and Israel. None of these countries confute or confirmed this[12]. **DoQu** is malware which had similar code base as Stuxnet. It is believed that Stuxnet and DoQu have same origin and same authors. Operation Stuxnet and

DoQu are also in correlation in many sources. DoQu used same exploits as Stuxnet, but it has different purpose. It had purpose to gather information about victims, in other words its purpose was to spy infected PCs. DoQu was written in higher programming languages, which is unusual for malware, because most of malware is written either in assembler, C or eventually in C++, or in some of scripting languages as Python or Lua. DoQu was written in object oriented C, and it is believed that is was compiled using Microsoft Visual Studio 2008.

Flame is the most complex malware that have been seen. It was found in 2012. and most of computers was infected in Near and Middle East. It is also believed that was created by Israel and US secret services and military. This is modular malware, that can be controlled by attacker and he can add new modules remotely. With all its modules it can be 20MB large. Flame could spread over the USB port or by network. It used rootkit capability to hide itself on infected system. It had capability to record audio, video, skype calls, network activity, to steal files from hard disk and send to attacker. In the moment when antivirus companies gathered sample of Flame for analysis, Flame was destroyed remotely by attacker who send kill command, which destroyed all the instances of Flame malware. Flame is written in Lua and C++, and as Stuxnet and DoQu it had valid stolen certificate.

7. Conclusion

It has passed more than 25 years since first malware for PC came out. Malware evolved, but some of the principles remained the same. First malware Brain.A spread over floppy disks, Stuxnet - one of the most complex malware - spread over the USB drives.

Purposes and motives for malware creation changed from exhibitionism, over revenge and profit to espionage and sabotage. Profit is still great motivator for malware creation, and it will continue to be in future. Military purposes such as espionage and sabotage were proven as success for malware creators. We can expect more of military malware and cyber warfare in future, since it is quite safe for attackers and can cause same damage as military attacks with all its fire power. It has to be seen how antivirus companies would deal with this kind of attackers with almost limitless resources for malware creation on one field and profit wanting malware creators on the other field. Still we might see some other purpose of malware creation in future in some game changing event such was Stuxnet when we are talking about military use of malware.

8. Works cited

- [1] Wikipedia, *Malware*, Internet: <http://en.wikipedia.org/wiki/Malware>, 03.02.2013.
- [2] Brain: Searching for first PC Virus, Mikko Hypponen, F-Secure, 2011.
- [3] *Malware: Fighting Malicious Code*, Ed Skoudis, Lenny Zeltser, Prentice Hall PTR, 2003
- [4] Wikipedia, Storm Worm, Internet: http://en.wikipedia.org/wiki/Storm_Worm, 10.02.2013.
- [5] Virus Wikia, Dark Avanger's Mutation Engine, http://virus.wikia.com/wiki/Dark_Avenger_Mutation_Engine, 17.02.2013.
- [6] Virus creation laboratory documentation, Internet, <http://www.textfiles.com/virus/DOCUMENTATION/vcl.txt>
- [7] One_half, ESET Threat encyclopedia, Internet <http://go.eset.com/us/threat-center/encyclopedia/threats/onehalf/>
- [8] Concept.A, FSecure Threat description, Internet, <http://www.f-secure.com/v-descs/concept.shtml>
- [9] Marburg, FSecure Threat description, Internet, <http://www.f-secure.com/v-descs/marburg.shtml>
- [10] Dressler, J. (2007). "United States v. Morris". *Cases and Materials on Criminal Law*. St. Paul, MN: Thomson/West
- [11] Slammer, FSecure Threat description, Internet, <http://www.f-secure.com/v-descs/mssqlm.shtml>
- [12] Stuxnet dossier, Symantec, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf



VIRUSES →

How to Find and Remove Viruses on Android Phones or iPhones

Does your phone have a virus? Can iPhones even get viruses? Discover how to scan and remove mobile malware from your Android or iPhone, get rid of malicious apps, and banish annoying pop-ups. Learn about the biggest risks to your phone and install our free anti-malware mobile app to start defending yourself from threats today.





Install free AVG AntiVirus

Get it for PC, iOS, Mac



2020
Top
Rated
product



2020
Top
Rated
product



Editor's
Rating
Excellent



f

twitter

in

envelope

How do you know if your phone has a virus? It doesn't – there's no such thing as viruses on Android or iPhone viruses. But phones can definitely get other [forms of malware](#). If your phone is showing the typical [symptoms of a malware infection](#), learn to get rid of malware manually or use a [virus removal tool](#) – or an anti-malware scanner – to clean it up automatically.

Read on for Android virus removal tips, or skip down to learn [how to remove an iPhone virus](#). Then, find out how to use a malware cleaner to remove malicious apps and run a phone virus scan. If you're dealing with a virus or malware on your PC or Mac, don't miss our expert guide to [removing malware from your computer](#).

Contains:

- How to remove a virus from an Android phone
- How to remove a virus from an iPhone
- How do I know if my phone has a virus?

→ Can Android phones get viruses?

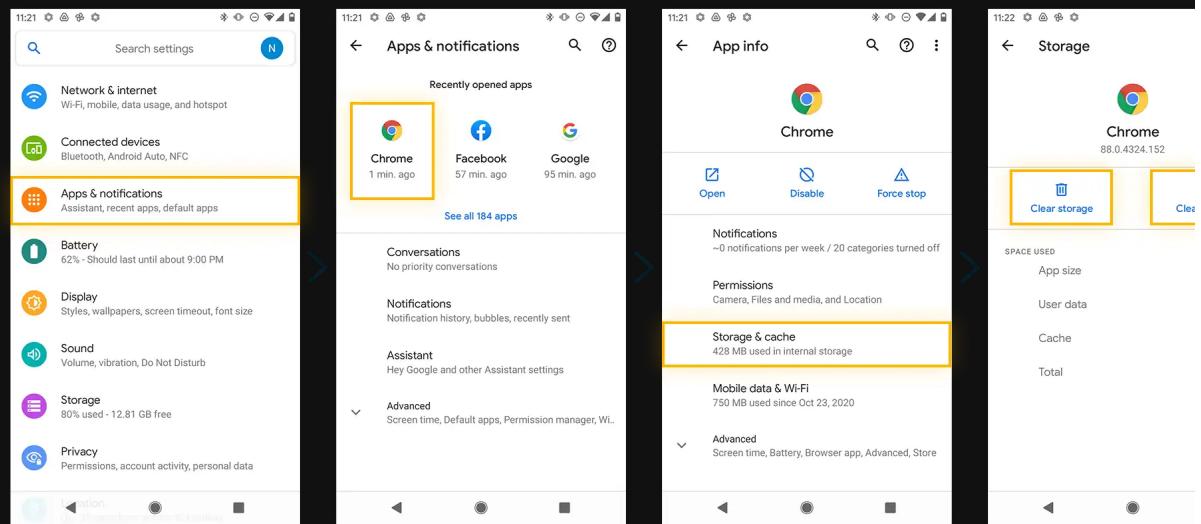
→ Can iPhones get viruses?



How to remove a virus from an Android phone

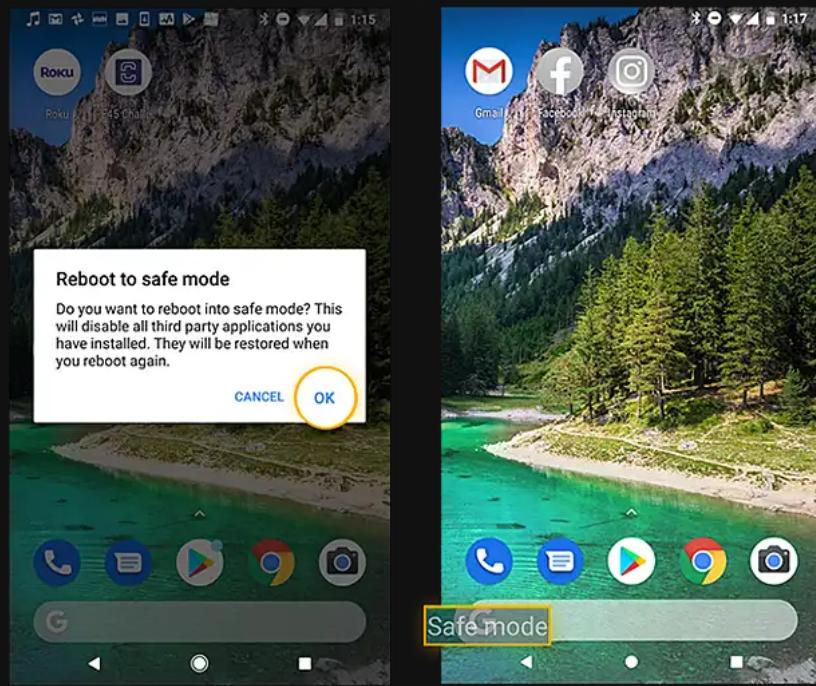
1. Clear your cache and downloads.

Open your **Settings**, go to **Apps & notifications**, and select Chrome. In the **Storage &** menu, follow the steps to clear your cache and storage.



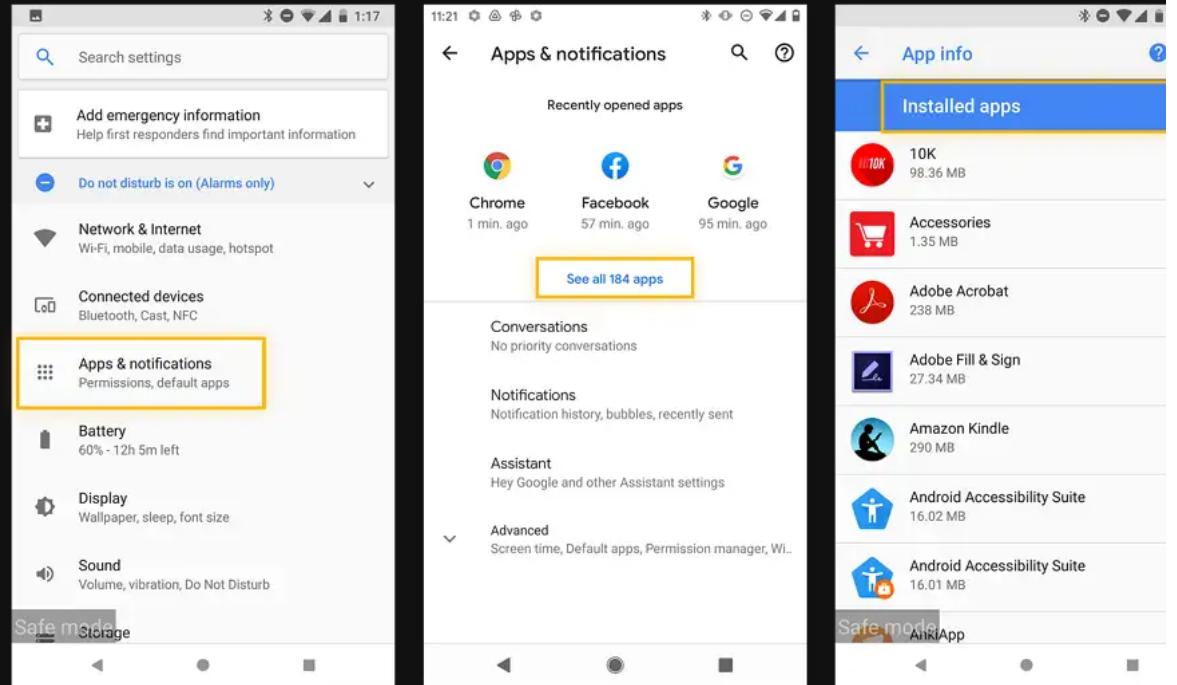
2. Restart your Android device in safe mode.

Press and hold the power button, then choose to restart your phone in safe mode. You can find **Safe Mode** in the corner of your screen after your phone reboots.



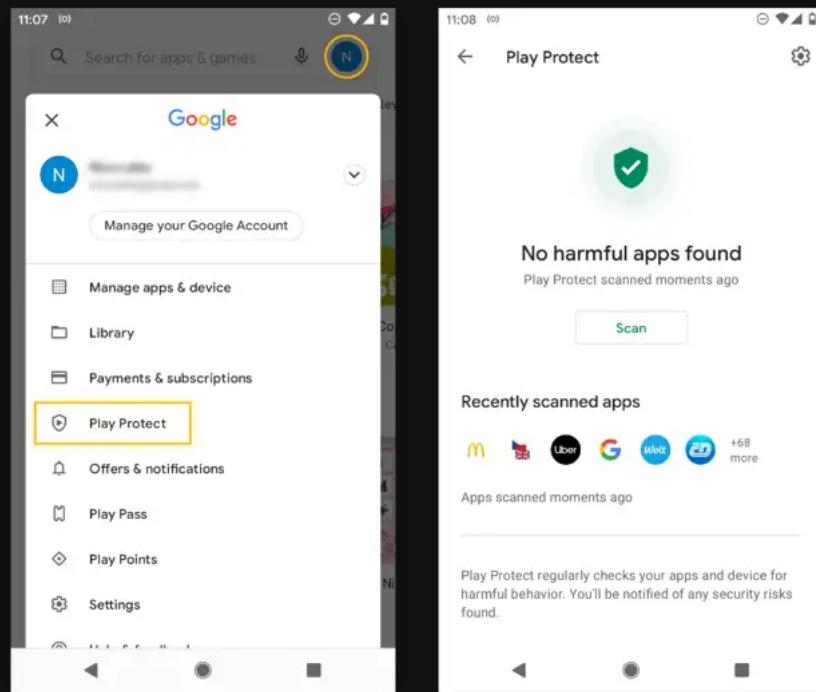
3. Find and remove malicious apps.

Open your **Settings** and tap **Apps & notifications**. Then tap **See all apps**. On the next screen, select **Installed apps** in the drop-down menu. Review your installed apps and look for those that are suspicious or unfamiliar, then uninstall them. Restart your phone when you're done.



4. Activate Google Play Protect.

The Play Protect feature in the Google Play Store monitors your apps for unusual behavior that can indicate the presence of Android malware. Open the Play Store app, tap your profile or avatar on the top right, and activate Play Protect in the menu.



5. Install anti-malware software.

An antivirus app is the best way to automatically detect and remove malware from your Android phone while preventing future infections. Install [AVG AntiVirus for Android](#) to keep your Android malware-free in real time.



Install free AVG AntiVirus

Get it for PC, iOS, Mac

The infographic below shows the steps you need to take to clear malware from your phone.

How to remove a virus from an Android phone



01 Clear your cache and downloads

Android adware can hide in your browser.

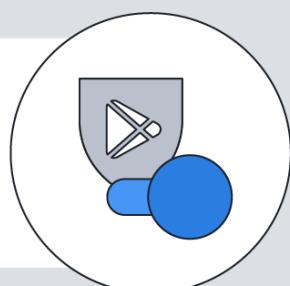
02 Restart in safe mode

Safe mode prevents malicious apps and other malware from running.



03 Find and remove malicious apps

Get rid of suspicious apps to get rid of malware.



04 Activate Google Play Protect

Google can detect malicious behavior in Android apps.



05 Install anti-malware software

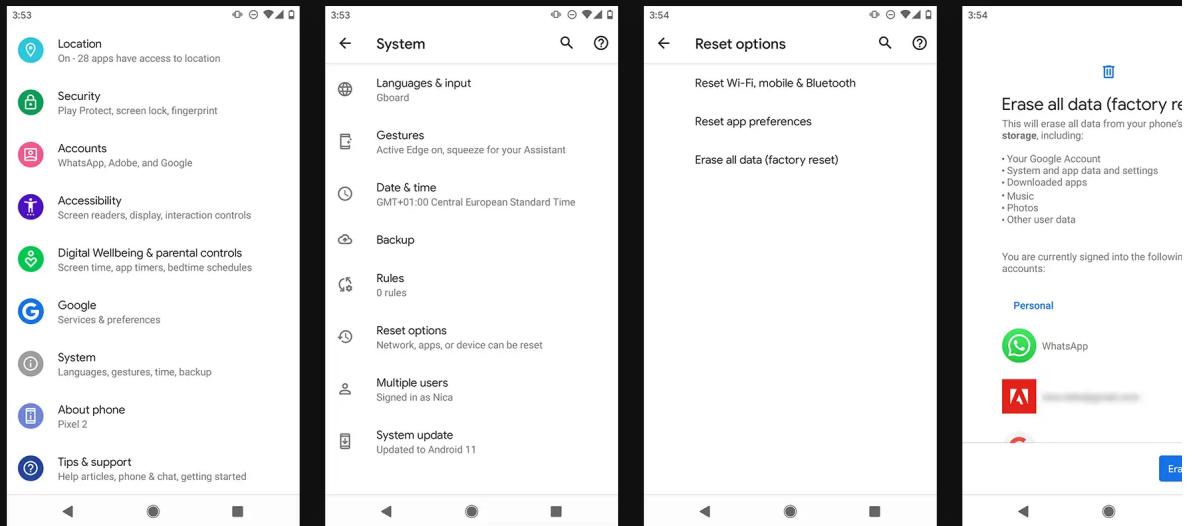
An antivirus will remove malware and prevent it in the future.

Last resort: wipe your Android

If the steps above don't work, try resetting your phone to its factory default settings. But this is a last resort – so before resetting your phone, try using an [Android virus removal app](#) instead. Otherwise, here's how to factory reset your Android:

1. Reset your phone.

Open up your **Settings**, select **System**, then tap **Reset options**. Choose **Erase all data (factory reset)** and then tap **Erase all data**. Confirm via the pop-up and restart your phone.



2. Restore your phone.

If you have a backup available, you can restore your phone to get your data back. You can restore from a backup from before your phone started acting strangely, otherwise you risk installing the Android malware again.

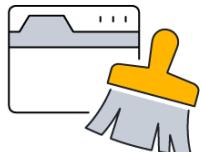
How to remove a virus from an iPhone

A lot of apparent iPhone malware is actually caused by **hackers manipulating your browser**. So clearing your browsing history and data should resolve iPhone virus issues. If not, try

restarting your phone, updating iOS, restoring your phone to a previous backup, or performing a factory reset.

Check out our infographic for the steps you need to take to remove iPhone malware, or skip down to see the steps explained in more detail.

How to remove a virus from an iPhone



01 Clear browsing history and data

Remove browser-based malware by resetting your browser.



02 Restart your phone

Sometimes you just need a quick reset.



03 Update to the newest iOS

Updating to the latest OS will help fix security issues.



04 Restore to a backup

Go back to before your problems started.



05 Factory reset your phone

If nothing is working, a factory reset can make your phone like new.

06 Install an iOS security app

Protect your phone from future digital threats.

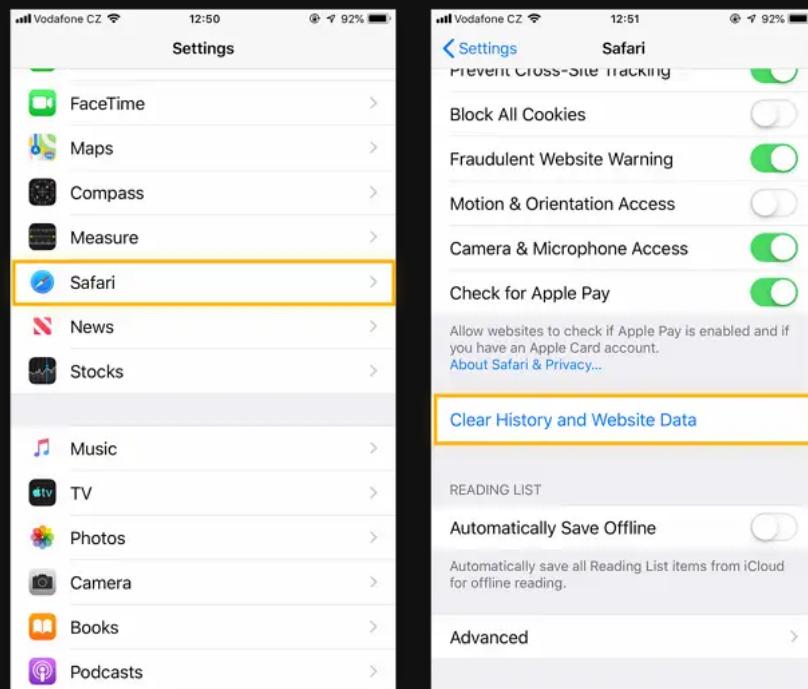


If you think your iPhone has a virus, here are a few ways to fix it:

1. Clear browsing history and data.

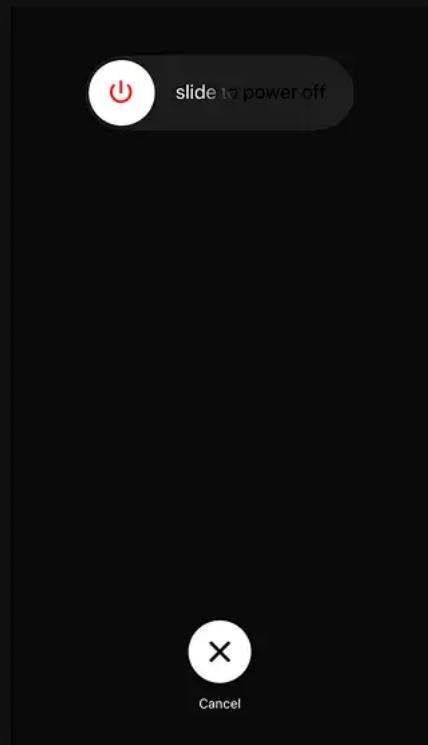
Go to **Settings** and scroll down to the **Safari** tab. Then tap **Clear History and Website Data**.

Repeat this process for any other browsers you use.



2. Restart your phone.

Hold the power button, turn your phone off, then turn it back on.

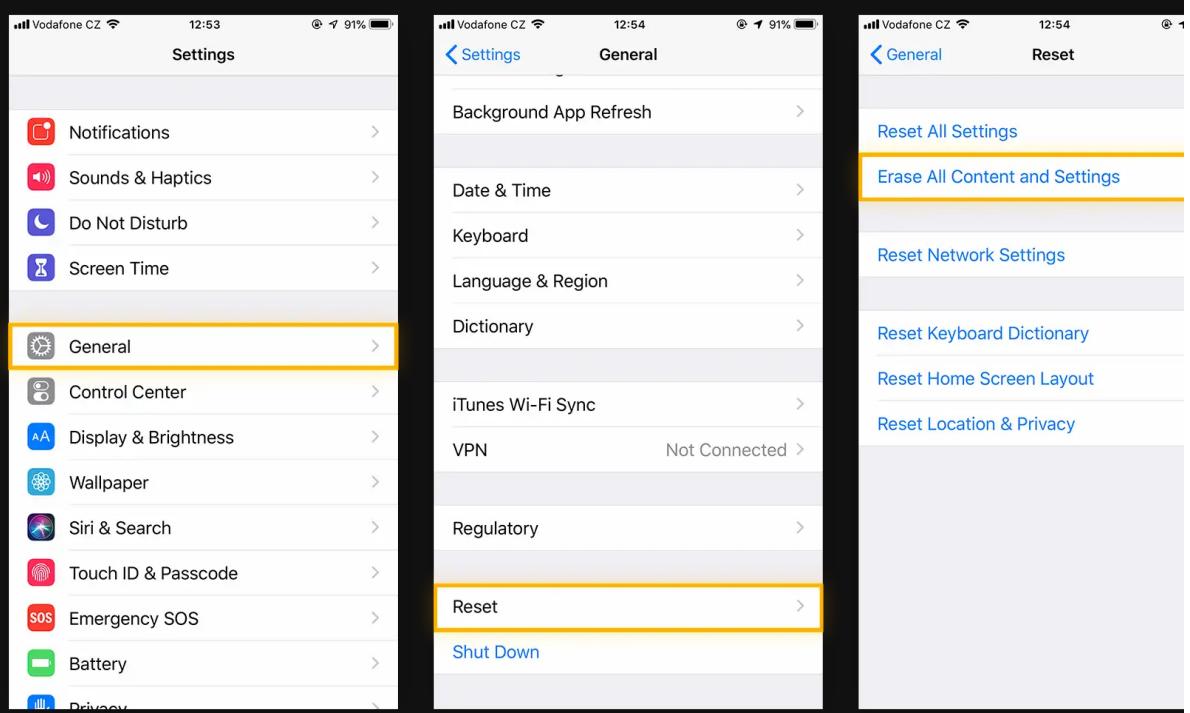


3. Update iOS.

Go to **Settings > General > Software Update**. If you see a software update, install it.

4. Restore your iPhone to a previous backup.

Go to **Settings > General > Reset**, then choose **Erase All Content and Settings**. Follow the prompts to restore your iPhone from a backup. Choose a backup you created from before your phone began acting strangely.



5. Factory-reset your iPhone

If your iPhone is still acting up, go to **Settings** > **General** > **Reset**, then choose **Erase Content and Settings**. Choose to reset your phone, rather than restore from a previous iCloud backup.

6. Install an iOS security app.

iOS is very secure, but you can make it even better with a dedicated security app. [AVG Mobile Security for iPhone and iPad](#) will make sure your passwords stay safe, your Wi-Fi network is secure, and your private photos stay private, even if your phone falls into the wrong hands.

It's easy to secure your Wi-Fi and protect your personal files with AVG Mobile Security.

Take your security up a level. Install [AVG Mobile Security for iOS](#) and start enjoying free, comprehensive protection for your iPhone or iPad today.



Install free AVG Mobile Security

How do I know if my phone has a virus?

Unusual behavior and unfamiliar apps are the two biggest warning signs of phone viruses and other malware. These signs will tell you if your iPhone or Android device has a phone virus.

- **Adware pop-ups:** Most ads can easily be blocked by [using an ad blocker](#) or with a [optimized browser](#) like [AVG Secure Browser](#), which comes with a built-in ad blocker. If you're seeing pop-up ads on your Android or iPhone even when your browser is closed, your phone could have [adware](#), which is a type of malware that spams you with extra ads.
- **Excessive app crashing:** Many apps crash periodically, but if your apps start crashing regularly for seemingly no reason, your phone could be infected with malware.
- **Increased data usage:** If you notice a sudden spike in data usage, that could be a sign that your phone has a virus. Malware is running background tasks on your device or transmitting information or [background data](#) from your phone. Remove the phone virus to help [control your mobile data usage](#).
- **Unexplained phone bill increases:** Some malware strains attack by sending premium text messages or SMS messages from your phone, causing your phone bill to skyrocket. [Ztorg Trojans](#) were found doing this in 2017, in addition to deleting incoming messages.
- **Your friends receive spam messages:** Some malicious software can hijack your messaging service and spam all your contacts with infected links. If your contacts tell you they received a weird message from your accounts, investigate right away.
- **Unfamiliar apps:** If you notice an app on your phone that you don't recall downloading or installing, it's probably been there for a while. Fake apps are a common symptom of malware on Android phones, and they should be uninstalled immediately. An anti-malware phone scanner will take care of this in a few quick taps.
- **Faster battery drain:** Malware mischief can use up a lot of energy, rapidly depleting your Android or iPhone battery. If your battery is dying faster than usual, malware might be the cause.

- **Overheating:** While the majority of the reasons your phone is overheating are normal and relatively harmless, it's also possible that the cause is a malware infection.

Can Android phones get viruses?

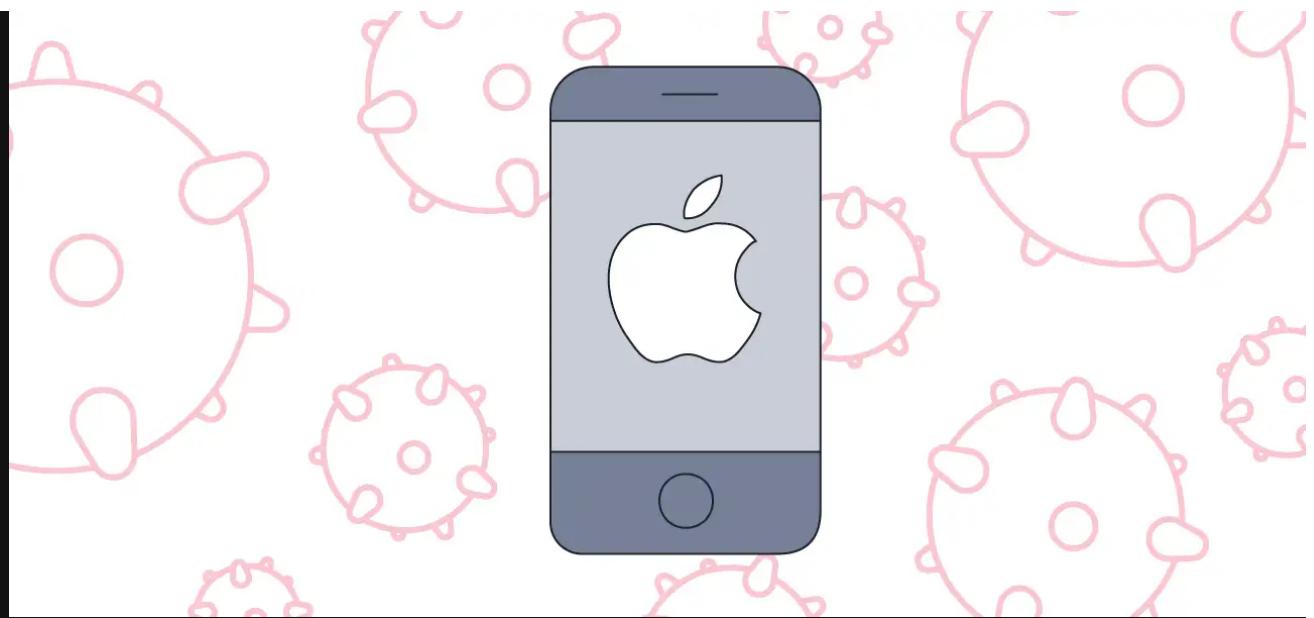
No, Android phones can't get viruses. But Android devices are vulnerable to other types of malware that can cause even more chaos on your phone. From malicious adware to spying apps and even Android ransomware, Android threats are widespread.

One of the reasons Android phones are susceptible to malware is because Android struggle with updates. Updates are important because they often contain critical security fixes to bugs or other vulnerabilities found in the operating system (OS).

Sourcing apps from third-party sources also increases the risk of accidentally installing malware. Android's open-source system and delayed rollout of updates are two major reasons why you should always use a strong antivirus solution for Android as an added layer of protection.

Can iPhones get viruses?

iPhones can't get viruses, because iPhone viruses don't exist. But while iPhones are less vulnerable to malware than Androids, there are other security threats you should watch out for. Phishing attacks and unsafe Wi-Fi networks are just two of the various threats that can affect your iPhone or iPad.



iPhone viruses don't exist (yet), but there are other threats to watch out for.

Jailbreaking your iPhone – when you remove Apple's built-in user restrictions – makes it just as vulnerable to malware as an Android device. So if you jailbreak your phone, it's important to learn how to do a virus scan for your iPhone. But even without jailbreaking your phone, iPhone users are still vulnerable to other serious security threats – like [identity theft](#).

A well-known 2021 iPhone hack installed [spyware](#) known as Pegasus that can steal tons of personal data and turn your phone into a permanent surveillance device. Using a [security exploit](#) to leverage a vulnerability in iMessage, Pegasus bypasses iOS 14's built-in security measures intended to prevent this tactic. The hack was created by Israel's NSO Group, one of the world's best hacking groups.

That's why we strongly recommend using a robust mobile protection app for iPhones and iPads. [Avast Mobile Security for iOS](#) goes way beyond antivirus or malware protection, keeping you safe every time you go online with free, innovative tools specially designed for your iPhone and iPad.

What can viruses do to your phone?

- Increase your data usage and rack up unexpected charges by sending spam or premium SMS messages, or subscribing you to unauthorized or premium apps or services.
- Spam you with ads that generate revenue for the attacker.

- Install rootkits that give hackers a “backdoor” to your phone.
- Record phone conversations and send them to hackers.
- Collect personal information, including your GPS location, contact lists, photos, email address, or banking details.
- Record your login credentials, including your passwords.
- Take over your device through rooting.
- Infect you with ransomware, locking you out of your files.

Before you install a new app, check if it's safe. Read both user and professional reviews to learn what other people think. Some apps might be clean when you download them, but later get infected with malware through updates – so it's important to stay alert.

How to protect against phone viruses

- **Download apps from trusted sources.** Google and Apple both vet apps for security before allowing them into their stores. Avoid third-party app stores, and don't jailbreak your iPhone or root your Android phone.
- **Check apps for safety.** Malicious apps occasionally find their way onto the official app stores, despite their security precautions. You should always check apps for safety before downloading them. Review the developer profile, read user reviews, and check the download count. Be extra careful when downloading anything brand-new, and don't download from questionable developers.
- **Research before you install.** User reviews are great, but you can also see what the press has to say. Consult expert reviews and independent evaluations of any new app before putting it on your phone.
- **Keep your phone updated.** Software providers often issue updates to fix bugs and plug security holes. Always update your phone's operating system and apps with the latest versions.
- **Don't click suspicious links.** Suspicious links in emails, text messages, or on social media can contain malware. Don't click on any links you don't expect to be there.

- **Be careful on public Wi-Fi.** Unsecured public Wi-Fi networks make it easy for hackers to intercept your traffic. Avoid doing anything sensitive on public Wi-Fi unless you're using a VPN.
- **Use cybersecurity protection.** Whether you have an Android or iPhone, a security app can help protect you against malware, phishing, and other mobile threats.

Protect your phone or tablet the easy way

We use our smartphones constantly. And they hold intimate details about our life. Don't let hackers in — build strong walls around your smartphone castle with a robust security and privacy app.

With AVG's cybersecurity protection, you can prevent adware, spyware, phishing, unsafe Wi-Fi networks, and a host of other mobile threats. Download [AVG AntiVirus for Android](#) or [AVG Mobile Security for iPhone and iPad](#) today for the free protection that millions of people all around the world trust every day.



[Install free AVG AntiVirus](#)

Get it for PC, [iOS](#), [Mac](#)

FAQs

What is a virus?

Viruses are a type of malware designed to infect computer systems and use the resources of their host machine to self-replicate and spread to other devices. Viruses were one of the first computer threats to emerge, and despite the rapid growth of other forms of malware in recent years, hackers continue to develop new viruses to exploit vulnerabilities in computer systems.

How can I scan my phone for viruses?

Use [AVG Antivirus for Android](#) or another dedicated [malware and virus removal tool](#) to scan your device from top to bottom, find and remove all kinds of malware threats (including adware, spyware, and [Trojans](#)), and stop malware from infecting your device again.

Can my phone get a virus from a website?

The chance of a website infecting your mobile device with a virus is low, but it is possible. And without a top [Android](#) or [iPhone](#) security app, other forms of malware designed to target specific [security exploits](#) pose a real threat. To browse securely, protect your device with a mobile security app and always follow [website safety](#) guidelines.

Does Google or Apple send virus warnings?

Neither Apple nor Google send virus warnings. If you receive [spoofed](#) notifications, emails, or other virus warnings supposedly from Apple or Google, these are [scareware](#) tactics designed to use [social engineering](#) to manipulate you into inadvertently downloading [malware](#), revealing personal information, or handing over your money.

Can hackers see through my phone camera?

Certain types of [spyware](#) and other malicious software tools can let hackers access your phone camera and other parts of the device – potentially letting them spy on you in real time. Protect yourself with a dedicated [anti-spyware](#) tool, and avoid falling prey to snoops by browsing safely on public Wi-Fi networks.

Does resetting a phone remove viruses and other malware?

Simply restarting your phone won't wipe malware from your device, but restoring your device to its factory settings probably will. If you're going to factory reset your device, back up your data to avoid losing it all. If you restore your phone from a backup, previously infected files could continue to infect your restored device. Use a [malware and virus removal tool](#) and [clear your phone's cache](#), [delete your cookies](#), and [clear your browsing history](#) to get rid of any lingering harmful internet files.



by **Nica Latto & Caroline Corrigan** on October 8, 2021

Updated on July 27, 2022



MOBILE

Get Free Virus Removal

Install free AVG AntiVirus for Android to remove and prevent viruses and other threats. Protect your phone in real time.



Free install

Get it for PC, iOS, Mac

The Latest Security Articles

[What's the Difference Between Malware and Viruses](#)

[What Is Malware? The Ultimate Guide to Malware](#)

[Microsoft Defender vs. Full-Scale Antivirus](#)

[What Is Scareware? Telltale Signs & How to Remove It](#)

[What Is a Logic Bomb Virus and How to Prevent It](#)

More helpful tips...

[Can iPads Get Viruses? You Need to Know](#)

[How to Get Rid of a Malware on Your Computer](#)

[What Is a Macro Virus? Do I Remove it?](#)

[The Best Free Antivirus for 2022](#)

About AVG

[Profile](#)

[Media Center](#)

[Policies](#)

[Contact Us](#)

Home Products

[Free Antivirus](#)

[Download](#)

[Internet Security](#)

[Android Antivirus](#)

[Free Mac Antivirus](#)

[Secure VPN](#)

[Tune Up](#)

Customer Area

[Register Your License](#)

[Anti-Theft Login](#)

[Home Product](#)

[Support](#)

[Security &](#)

[Performance Tips](#)

[Online Research](#)

Partners & Business

[Business Antivirus](#)

[Software](#)

[Partner Support](#)

[Business Support](#)

[Affiliates](#)



Virus Scanning &
Malware Removal
Installation Files
Beta Downloads
Driver Updater
Battery Saver

[Log in to AVG MyAccount](#)

[Privacy](#) | [Report vulnerability](#) | [Contact security](#) | [License agreements](#) | [Modern Slavery Statement](#) | [Cookies](#) | [Accessi](#)

[Do not sell my info](#) | [Cookie preferences](#) | All third party trademarks are the property of their respective owners. | © 1

Avast Software s.r.o.

How to easily clean an infected computer (Malware Removal Guide)

Malware, short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses.

It's not always easy to tell if your computer was compromised or not, because these days cybercriminals are going to great lengths to hide their code and conceal what their programs are doing on an infected computer.

It's very difficult to provide a list of characteristic symptoms of a infected computer because the same symptoms can also be caused by hardware incompatibilities or system instability, however here are just a few examples that may suggest that your PC has been compromised :

- You may receive the error "Internet Explorer could not display the page" when attempting to access certain websites
- Your web browser (e.g., Microsoft Internet Explorer, Mozilla Firefox, Google Chrome) freezes, hangs or is unresponsive
- Your web browser's default homepage is changed
- Access to security related websites is blocked
- You get redirected to web pages other than the one you intended to go to
- You receive numerous web-browser popup messages
- Strange or unexpected toolbars appear at the top of your web browser
- Your computer runs slower than usual
- Your computer freezes, hangs or is unresponsive
- There are new icons on your desktop that you do not recognize
- Your computer restarts by itself (but not a restart caused by Windows Updates)
- You see unusual error messages (e.g., messages saying there are missing or corrupt files folders)
- You are unable to access the Control Panel, Task Manager, Registry Editor or Command Prompt.

This article is a comprehensive guide, which will remove most of malware infections that may reside on your computer. And if you are experiencing any of the above symptoms, then we strongly advise you follow this guide to check and remove any infection that you might have on your computer.

How to remove viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs

OPTIONAL: Some forms of malware will not allow you to start some of the below utilites and on-demand scanners, while running Windows in Normal mode. If this happens, we recommend that you start your computer in Start your computer in Safe Mode with Networking, and try from there to perform the scan.

We recommend that you first try to run the below scans while your computer is in Normal mode, and only if you are experiencing issues, should you try to start the computer in Safe Mode with Networking.

To start your computer Start your computer in Safe Mode with Networking, you can follow the below steps:

1. Remove all floppy disks, CDs, and DVDs from your computer, and then **restart your computer**.
2. **If you are using Windows XP, Vista or 7 press and hold the F8 key as your computer restarts.** Please keep in mind that you need to press the F8 key **before the Windows start-up logo appears**.
Note: With some computers, if you press and hold a key as the computer is booting you will get a stuck key message. If this occurs, instead of pressing and holding the “F8 key”, **tap the “F8 key” continuously** until you get the *Advanced Boot Options* screen. If you are using Windows 8, press the **Windows key + C**, and then click **Settings**. Click **Power**, **hold down Shift** on your keyboard and click **Restart**, then click on **Troubleshoot** and select **Advanced options**.
3. In the **Advanced Options** screen, select **Startup Settings**, then click on **Restart**.
4. If you are using Windows XP, Vista or 7 in the *Advanced Boot Options* screen, use the arrow keys to **highlight Safe Mode with Networking** , and then **press ENTER**.

```
Windows Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking ←
Safe Mode with Command Prompt

Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration (your most recent settings)
Directory Services Restore Mode (Windows domain controller)
Debugging Mode
Disable automatic restart on system failure

Start Windows Normally
Reboot
```

Use the up and down arrow keys to move the highlight to your selection.

If you are using Windows 8, press 5 on your keyboard to **Enable Safe Mode with Networking**.

Windows will start in Safe Mode with Networking.

STEP 1: Remove bootkits and trojans with Combofix

In this first step, we will run a system scan with Combofix to remove any malicious software that might be installed on your system.

1. Download Combofix from any of the below links.
[**COMBOFIX DOWNLOAD LINK #1**](#) (*This link will automatically download Combofix on your computer*)
[**COMBOFIX DOWNLOAD LINK #2**](#) (*This link will automatically download Combofix on your computer*)
2. Before running this utility ,please follow the below instructions:
 - o Close any open browsers.
 - o **Temporarily disable your anti-virus**, script blocking and any anti-malware real-time protection **before performing a scan**. They can interfere with ComboFix or remove some of its embedded files which may cause “*unpredictable results*”.
 - o Combofix will disconnect your machine from the Internet as soon as it starts. Please do not attempt to re-connect your machine back to the Internet until Combofix has completely finished.
If there is no internet connection after running Combofix, then restart your computer to restore back your connection.
3. To start the Combofix scan, double-click on ComboFix.exe and then follow the prompts.
You can watch the below video to see how to use Combofix:
Other important notes:

- **DO NOT** mouse-click Combofix's window while it is running. That may cause it to stall.
- If after the reboot you get errors about programs being marked for deletion then reboot, that will cure it.

STEP 2: Run RKill to terminate any malicious processes

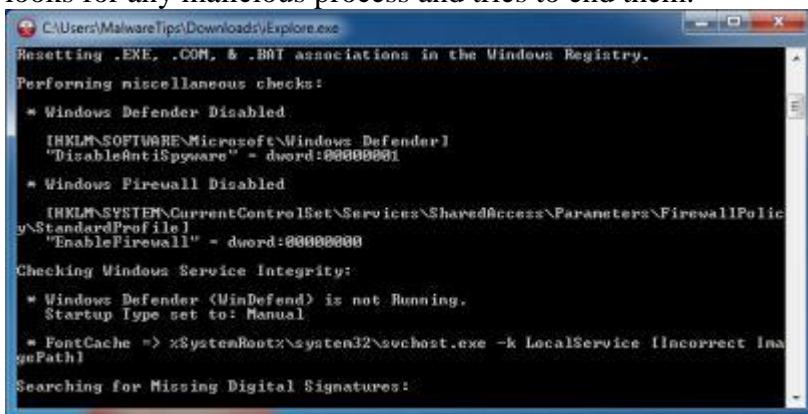
RKill is a program that will attempt to terminate all malicious processes that are running on your machine, so that we will be able to perform the next step without being interrupted by this malicious software.

Because this utility will only stops the running process, and does not delete any files, after running it you should not reboot your computer as any malware processes that are configured to start automatically will just be started again.

1. Please **download the latest official version of RKill**. Please note that we will use a renamed version of RKILL so that malicious software won't block this utility from running.
RKill DOWNLOAD LINK (*This link will automatically download RKILL renamed as iExplore.exe*)
2. Double click on **iExplore.exe** to start RKill and stop any processes associated with Luhe.Sirefef.A.



3. RKill will now start working in the background, please be patient while the program looks for any malicious process and tries to end them.



```
C:\Users\MalwareTips\Downloads\iExplore.exe
Resetting .EXE, .COM, & .BAT associations in the Windows Registry.

Performing miscellaneous checks:
* Windows Defender Disabled
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Defender]
"DisableAntiSpyware" - dword:00000001

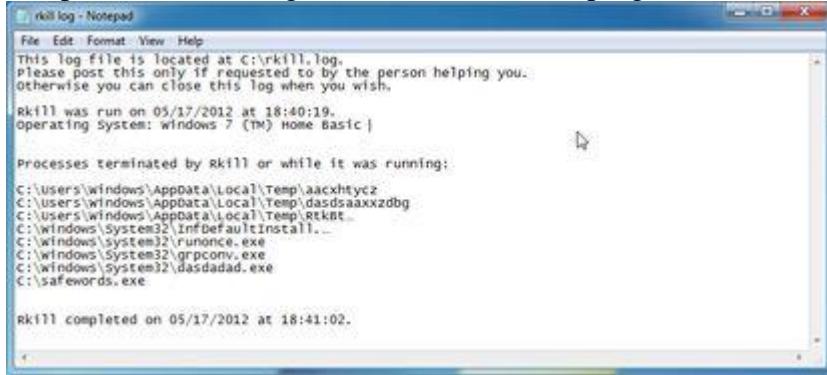
* Windows Firewall Disabled
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]
"EnableFirewall" - dword:00000000

Checking Windows Service Integrity:
* Windows Defender (WinDefend) is not Running.
  Startup Type set to: Manual

* FontCache => xSystemRoot\system32\svchost.exe -k LocalService [Incorrect ImagePath]

Searching for Missing Digital Signatures:
```

4. When the Rkill utility has completed its task, it will **generate a log**. Do not reboot your computer after running RKill as the malware programs will start again.



```
rkill log - Notepad
File Edit Format View Help
This log file is located at C:\rkill.log.
Please post this only if requested to by the person helping you.
Otherwise you can close this log when you wish.
rkill was run on 05/17/2012 at 18:40:19.
operating System: Windows 7 (TM) Home Basic |

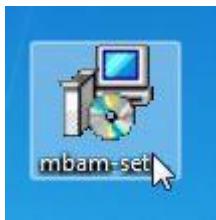
Processes terminated by Rkill or while it was running:
C:\Users\Windows\AppData\Local\Temp\aacxhtyc2
C:\Users\Windows\AppData\Local\Temp\dadsaaxx2dbg
C:\Users\Windows\AppData\Local\Temp\REKBT...
C:\Windows\System32\zinfDefaultInstall...
C:\Windows\System32\runonce.exe
C:\Windows\System32\grpcconv.exe
C:\Windows\System32\dasdadad.exe
C:\safewords.exe

rkill completed on 05/17/2012 at 18:41:02.
```

STEP 3: Remove Trojan Horses, rogue security software and other malicious files from your computer with Malwarebytes Anti-Malware Free

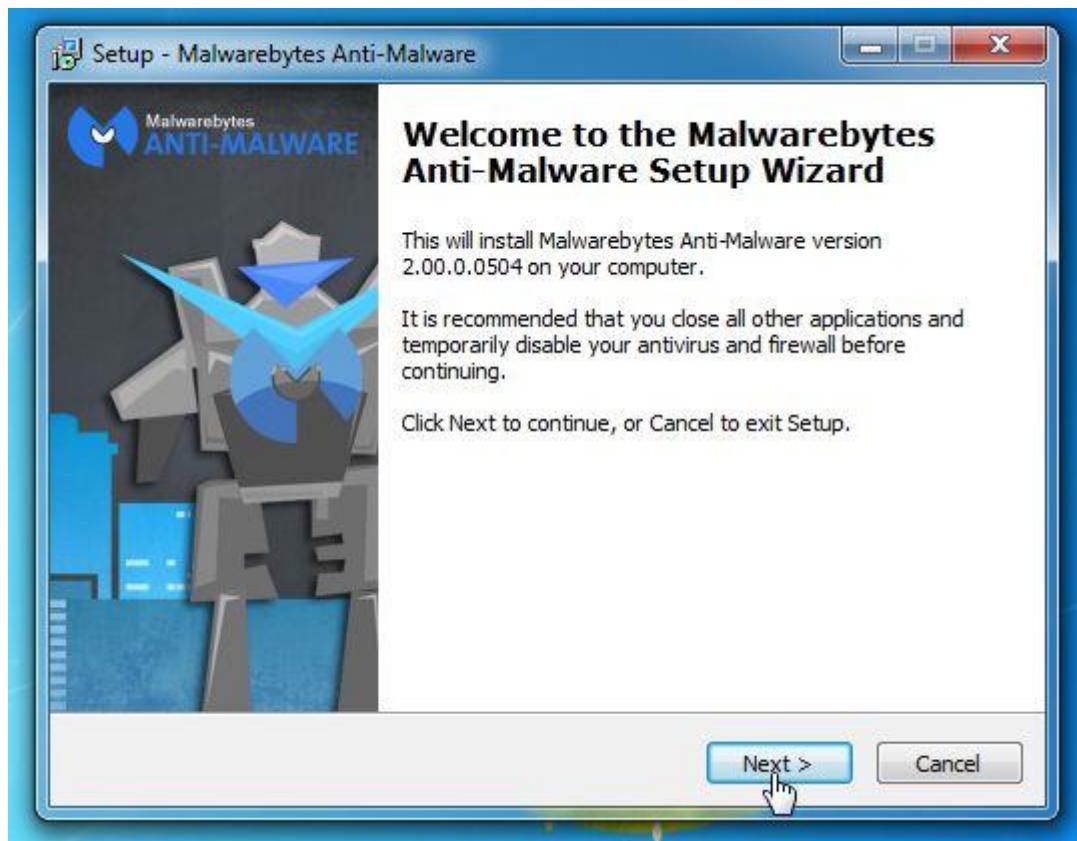
Malwarebytes Anti-Malware Free uses industry-leading technology to detect and remove all traces of malware, including worms, Trojans, rootkits, rogues, dialers, spyware, and more. It is important to note that Malwarebytes Anti-Malware works well and should run alongside antivirus software without conflicts.

1. You can download **Malwarebytes Anti-Malware** from the below link.
[**MALWAREBYTES ANTI-MALWARE DOWNLOAD LINK**](#) *(This link will open a new web page from where you can download Malwarebytes Anti-Malware Free)*
2. Once downloaded, close all programs, then double-click on the icon on your desktop named “mbam-setup-consumer-2.00.xx” to start the installation of Malwarebytes Anti-Malware.



💡 You may be presented with a User Account Control dialog asking you if you want to run this file. If this happens, you should click “Yes” to continue with the installation.

3. When the installation begins, you will see the *Malwarebytes Anti-Malware Setup Wizard* which will guide you through the installation process.



To install Malwarebytes Anti-Malware on your machine, *keep following the prompts* by

clicking the “**Next**” button.

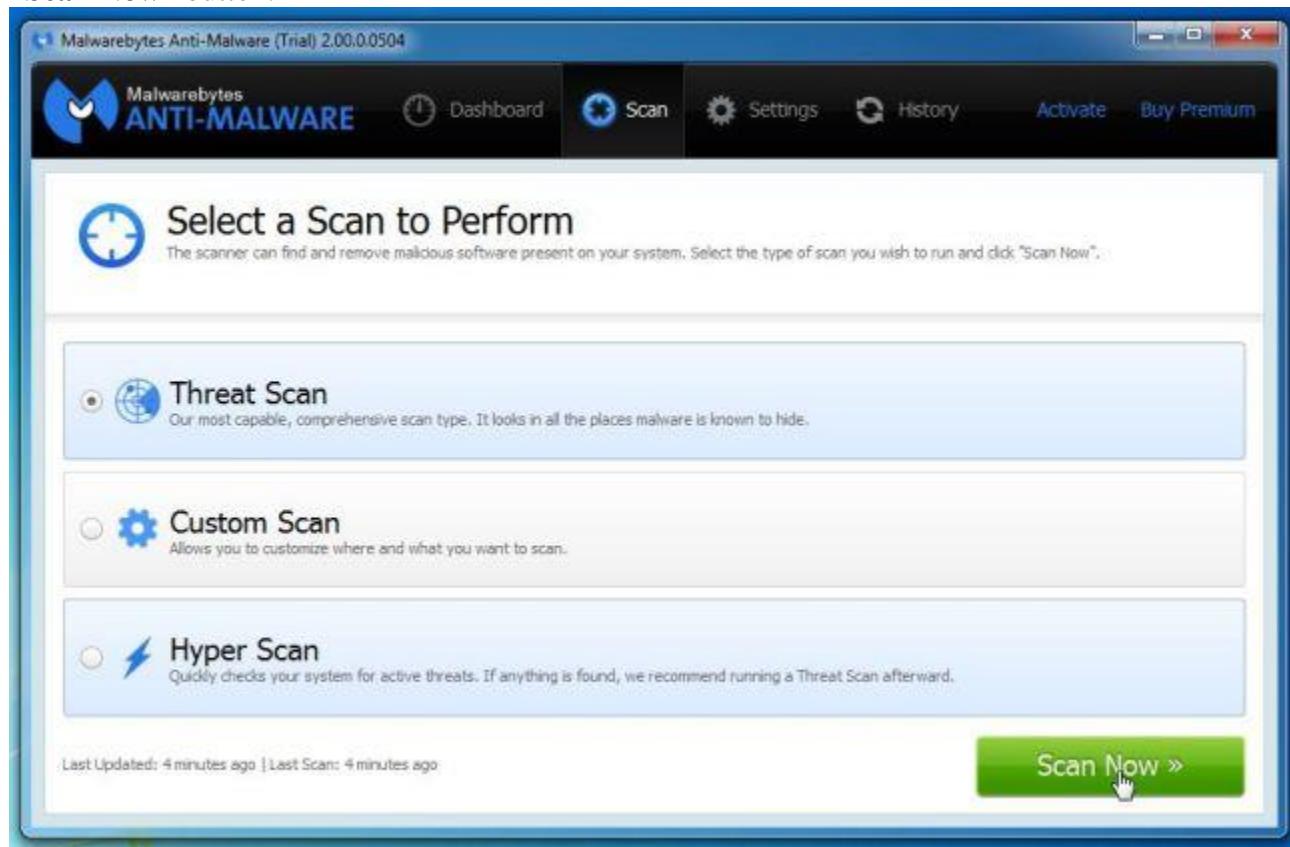


4. Once installed, Malwarebytes Anti-Malware will automatically start and you will see a message stating that you should update the program, and that a scan has never been run on your system. To start a system scan you can click on the “**Fix Now**” button.

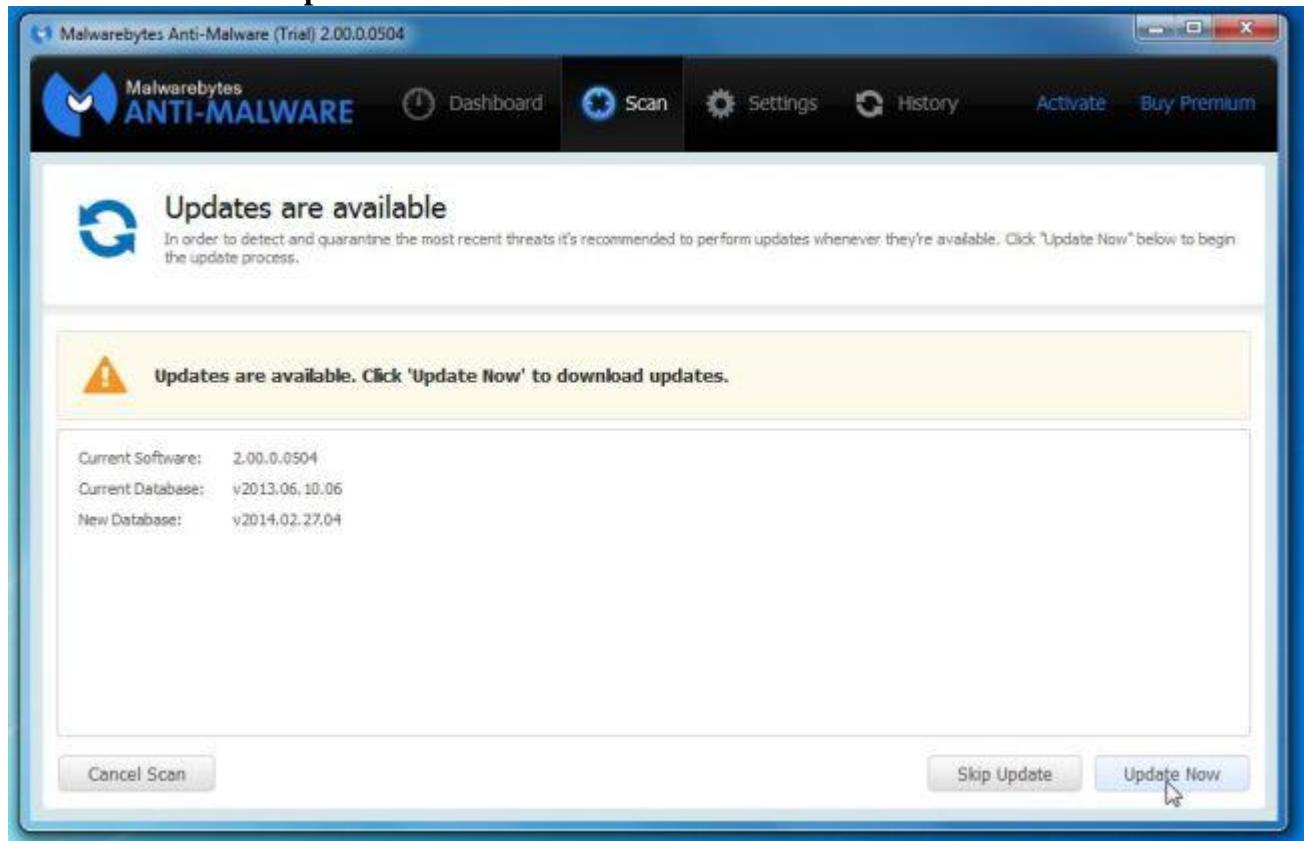


Alternatively, you can click on the “Scan” tab and select “*Threat Scan*”, then click on the

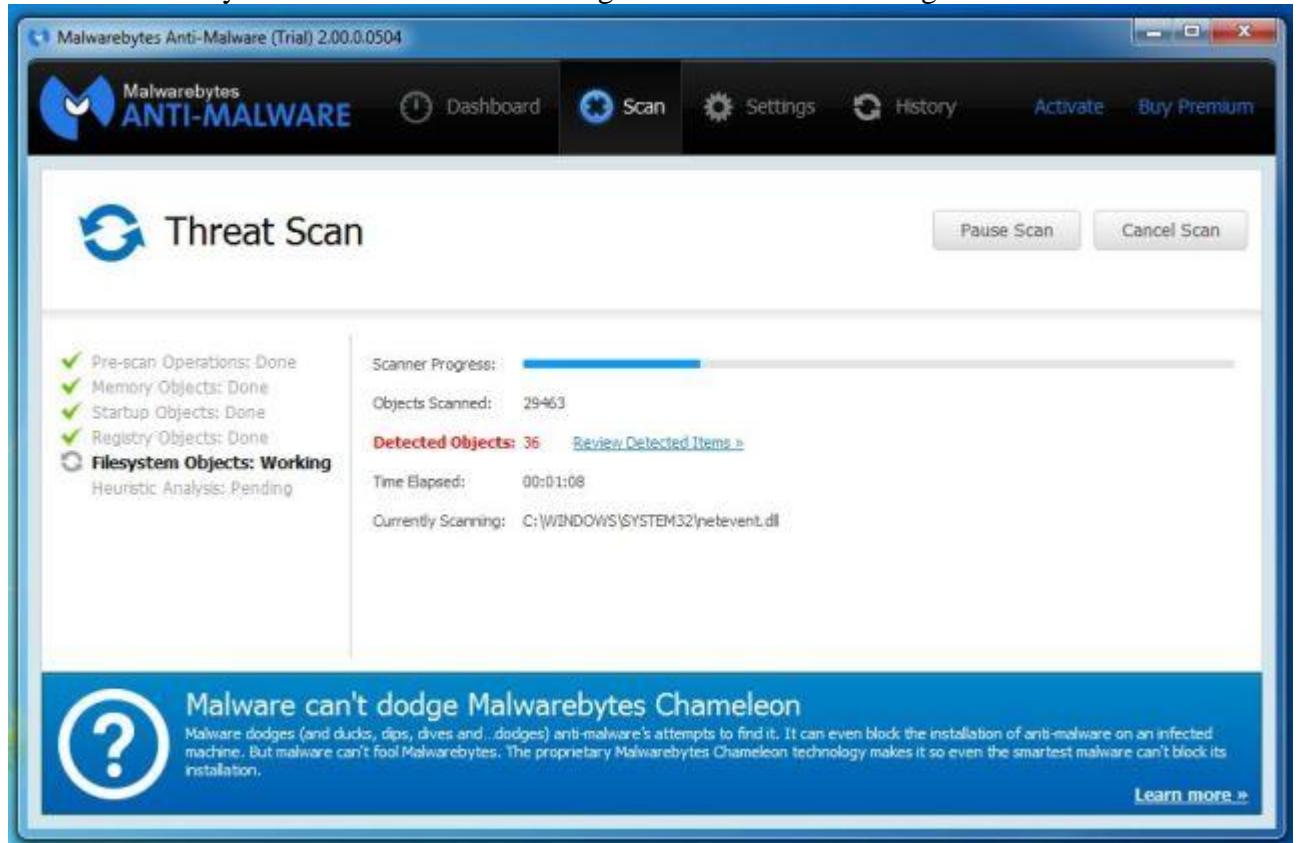
“Scan Now” button.



5. Malwarebytes Anti-Malware will now check for updates, and if there are any, you will need to click on the “**Update Now**” button.



6. Malwarebytes Anti-Malware will now start scanning your computer for the pop-up virus. When Malwarebytes Anti-Malware is scanning it will look like the image below.



7. When the scan has completed, you will now be presented with a screen showing you the malware infections that Malwarebytes' Anti-Malware has detected. To remove the malicious programs that Malwarebytes Anti-malware has found, click on the "Quarantine All" button, and then click on the "Apply Now" button.

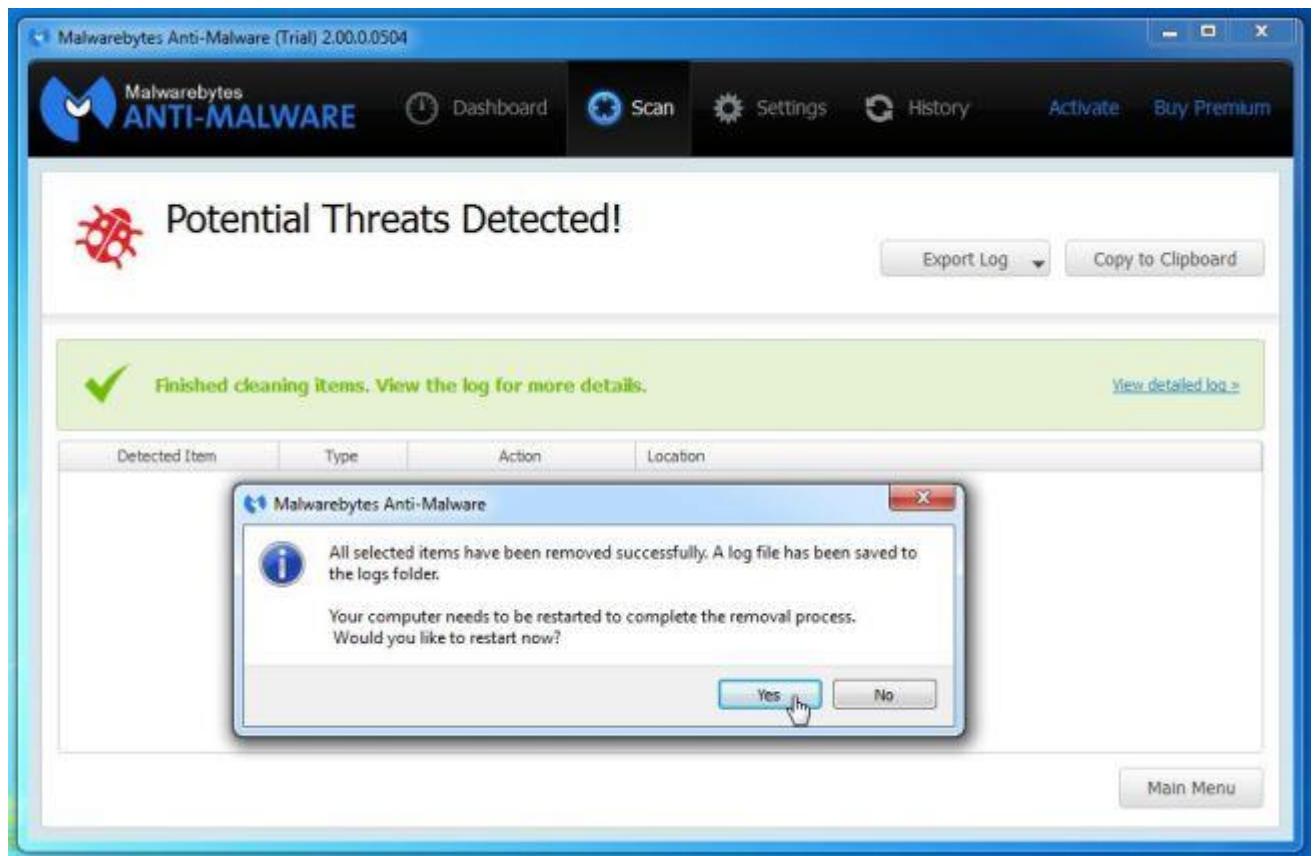
The screenshot shows the Malwarebytes Anti-Malware software interface. At the top, the title bar reads "Malwarebytes Anti-Malware (Trial) 2.00.0.0504". The main menu bar includes "Dashboard", "Scan", "Settings", "History", "Activate", and "Buy". A central message box displays "Potential Threats Detected!" with a red bug icon. Below it, a dialog box titled "Choose an action for the detected items!" lists the following detected items:

Detected Item	Type	Action	Location
Trojan.Zbot	File	Quarantine	C:\Users\MalwareTips\AppData\Roaming\Xaotko\yyf.exe
Trojan.Zbot	Registry Value	Quarantine	HKU\S-1-5-21-1758991082-695353234-2857450141-1000-{ED1FC765-E35E-4C
Trojan.Zbot	Process	Quarantine	C:\Users\MalwareTips\AppData\Roaming\Xaotko\yyf.exe
Backdoor.Agent.DCRSAGen	File	Quarantine	C:\Users\MalwareTips\Downloads\2014-02-25\2014-02-25\gg.exe
Backdoor.Agent.DCRSAGen	Process	Quarantine	C:\Users\MalwareTips\Downloads\2014-02-25\2014-02-25\gg.exe
Backdoor.Agent.DCRSAGen	Process	Quarantine	C:\Users\MalwareTips\Downloads\2014-02-25\2014-02-25\gg.exe
Virus.Skinin	File	Quarantine	C:\Users\MalwareTips\AppData\Roaming\Install\hkrmid.exe

Buttons at the bottom of the dialog box include "Quarantine All", "Cancel", and "Apply All". In the background, a message box says "Scan Complete - Malware Detected" with an exclamation mark icon, and a note: "Malwarebytes Anti-Malware has detected one or more threats. Click here to view results."

Please note that the infections found may be different than what is shown in the image.

8. Malwarebytes Anti-Malware will now quarantine all the malicious files and registry keys that it has found. When removing the files, Malwarebytes Anti-Malware may require a reboot in order to remove some of them. If it displays a message stating that it needs to reboot your computer, please allow it to do so.



After your computer will restart, you should open Malwarebytes Anti-Malware and perform another “Threat Scan” to verify that there are no remaining threats

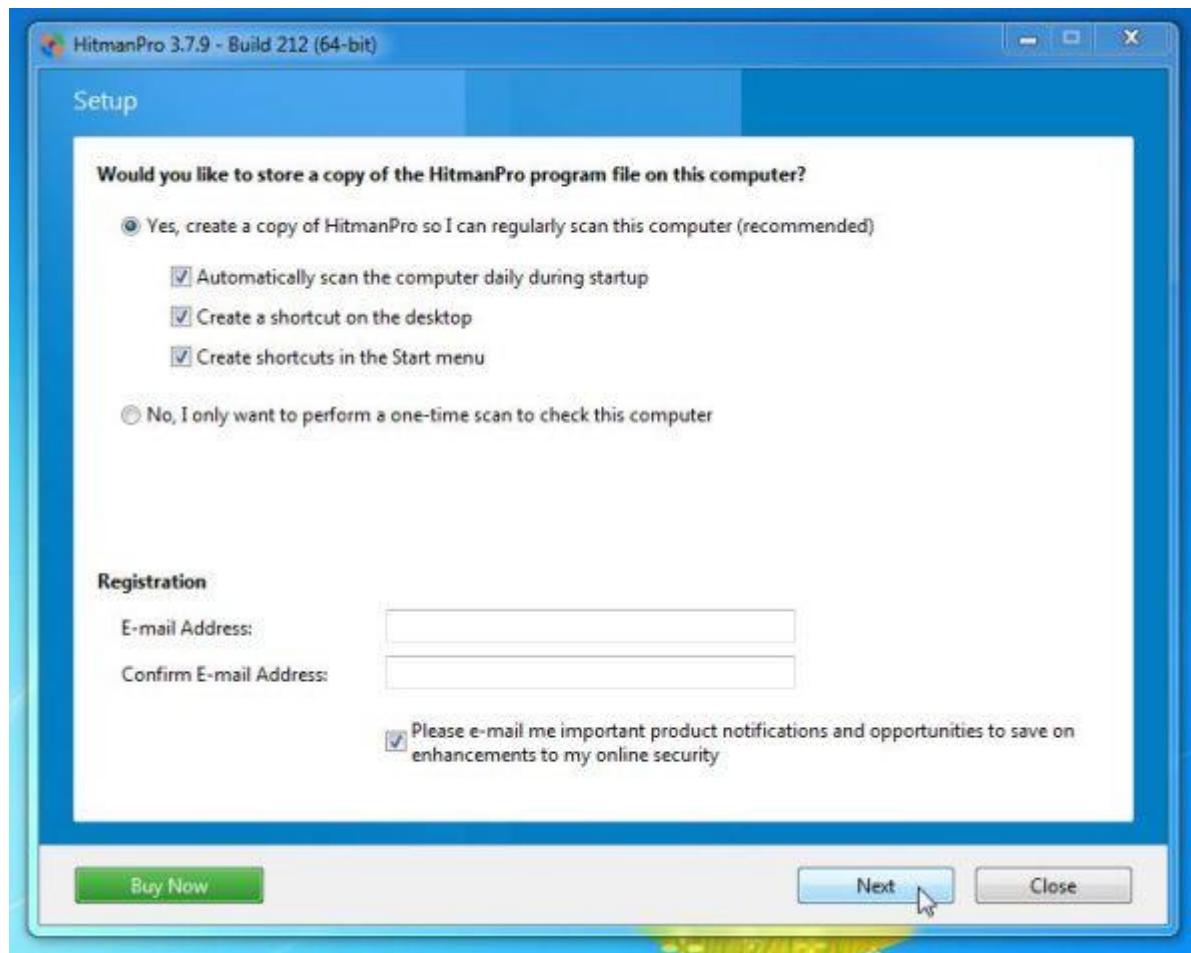
STEP 4: Remove stubborn rootkits from your computer with HitmanPro

HitmanPro is a second opinion scanner, designed to rescue your computer from malware (viruses, trojans, rootkits, etc.) that have infected your computer despite all the security measures you have taken (such as anti virus software, firewalls, etc.). HitmanPro is designed to work alongside existing security programs without any conflicts. It scans the computer quickly (less than 5 minutes) and does not slow down the computer.

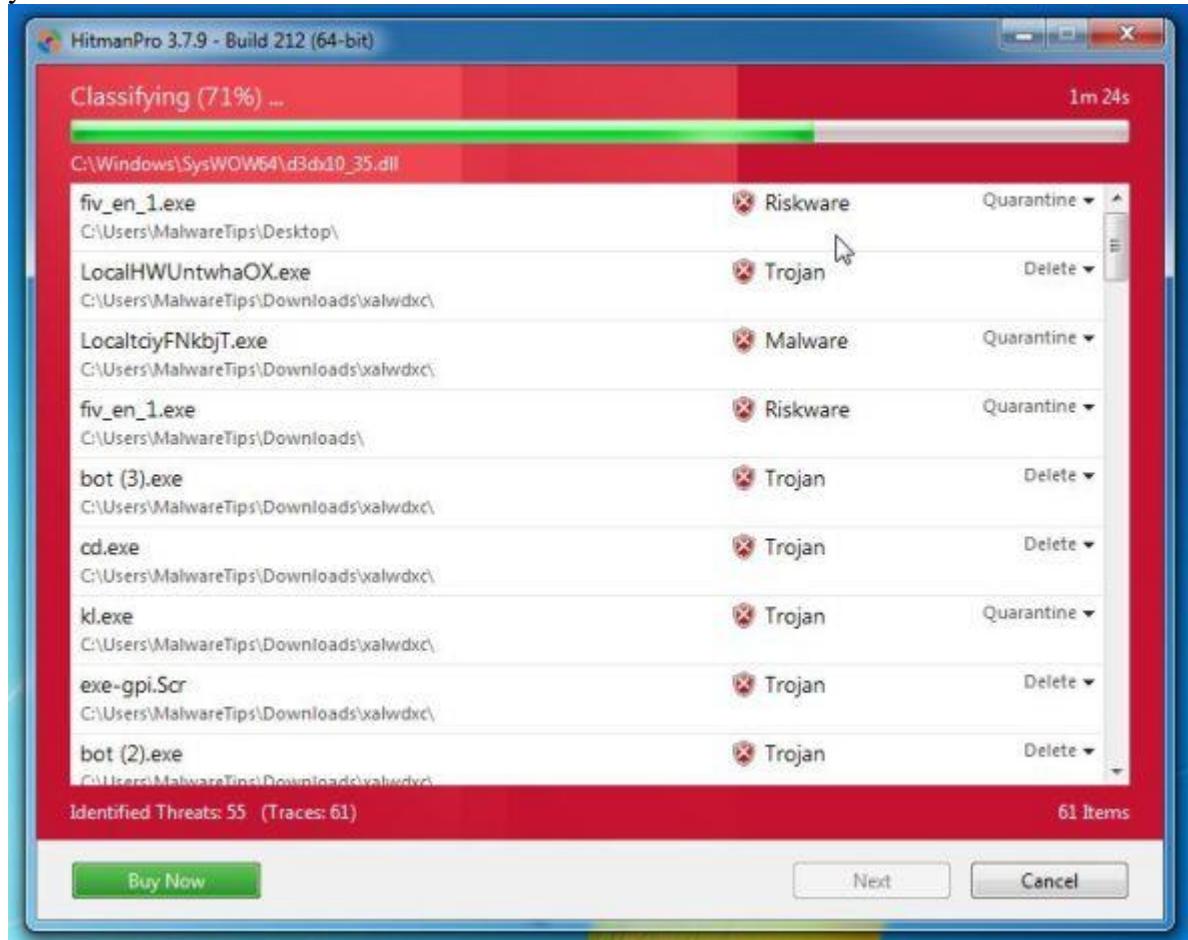
1. You can download **HitmanPro** from the below link:
[HITMANPRO DOWNLOAD LINK](#) (*This link will open a new web page from where you can download HitmanPro*)
2. Double-click on the file named “**HitmanPro.exe**” (for 32-bit versions of Windows) or “**HitmanPro_x64.exe**” (for 64-bit versions of Windows). When the program starts you will be presented with the start screen as shown below.



Click on the “**Next**” button, to install HitmanPro on your computer.

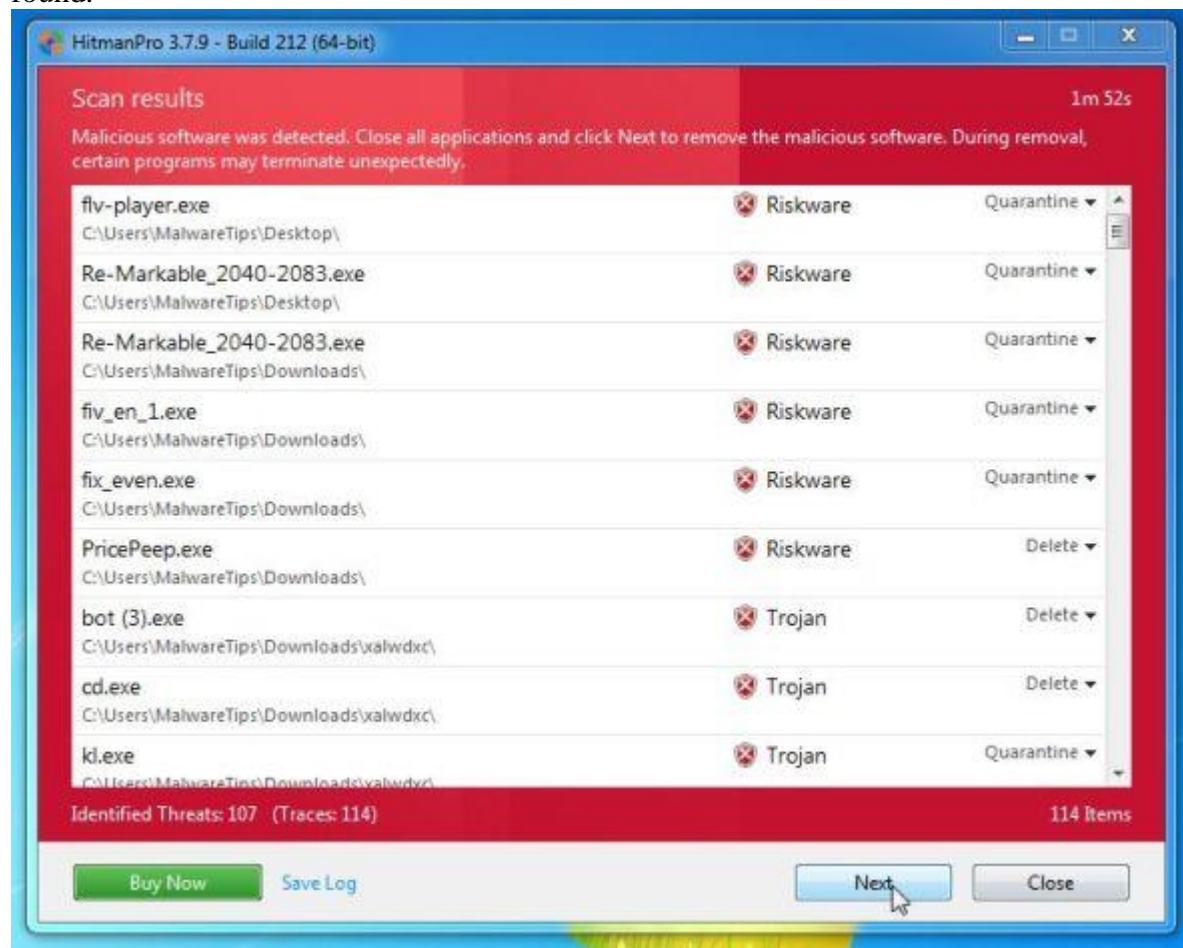


3. HitmanPro will now begin to scan your computer for any malicious files that may be on your machine.

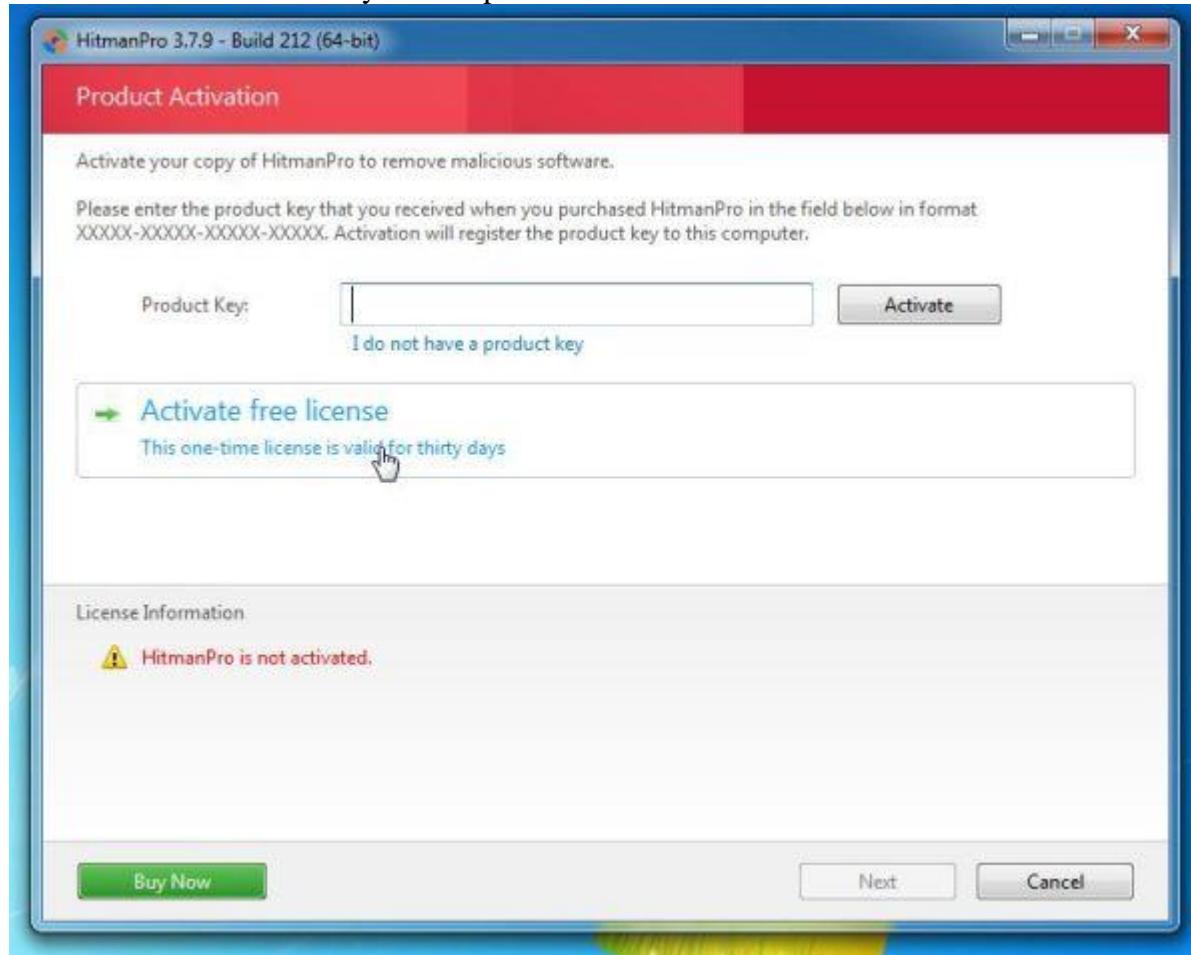


4. When it has finished it will display a list of all the malware that the program found as shown in the image below. Click on the “Next” button, to remove any virus that has been

found.



5. Click on the “Activate free license” button to begin the **free 30 days trial**, and remove all the malicious files from your computer.

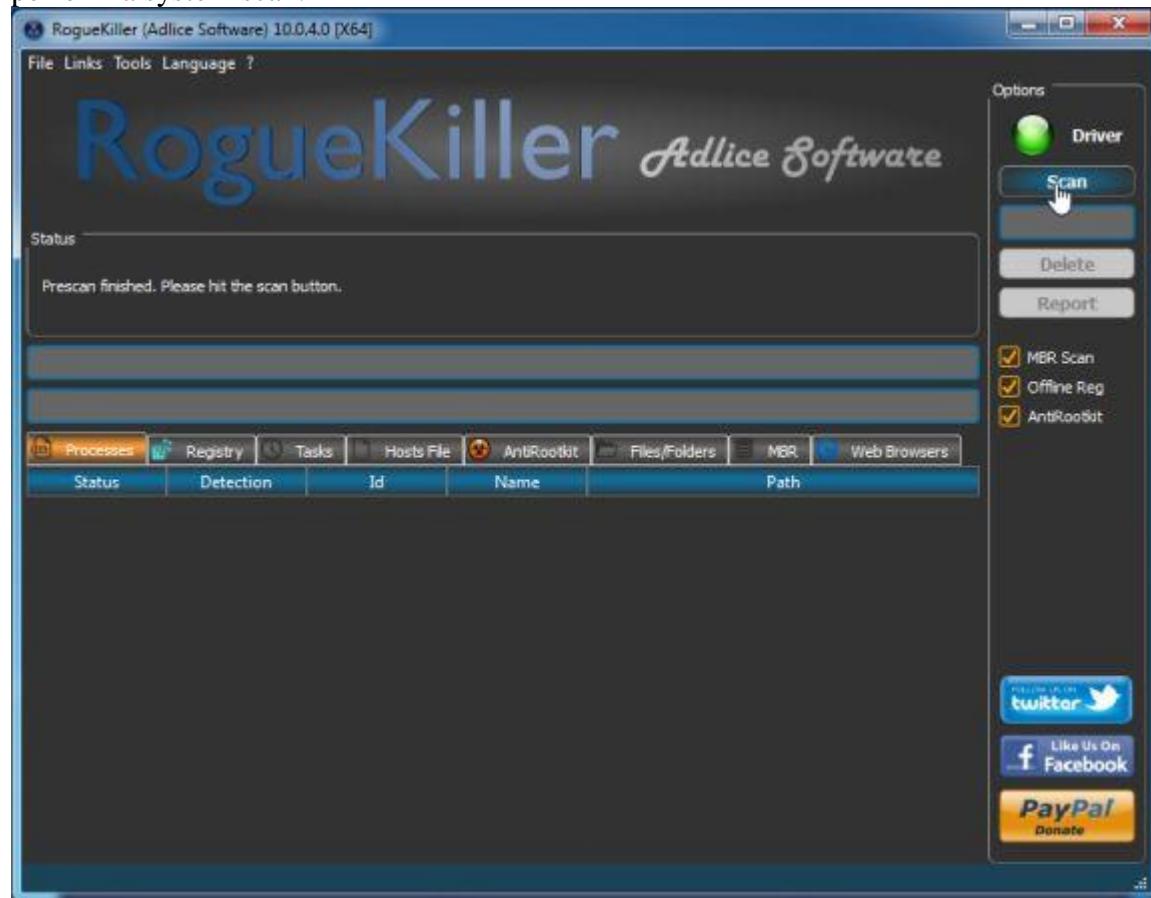


STEP 5: Remove the malicious registry keys added by malware with **RogueKiller**

RogueKiller is a utility that will scan for the unwanted registry keys and any other malicious files on your computer.

1. You can download the latest official version of **RogueKiller** from the below links.
 - o [**ROGUEKILLER x86 DOWNLOAD LINK**](#) (*For 32-bit machines*)
 - o [**ROGUEKILLER x64 DOWNLOAD LINK**](#) (*For 64-bit machines*)
2. Double-click on the file named “**RogueKiller.exe**” (for 32-bit versions of Windows) or “**RogueKillerX64.exe**” (for 64-bit versions of Windows). **Wait for the Prescan to complete.** This should take only a few seconds, then click on the “**Scan**” button to

perform a system scan.



3. After the scan has completed, click on the “Delete” button to remove Trojan.Poweliks!gm malicious registry keys or files.

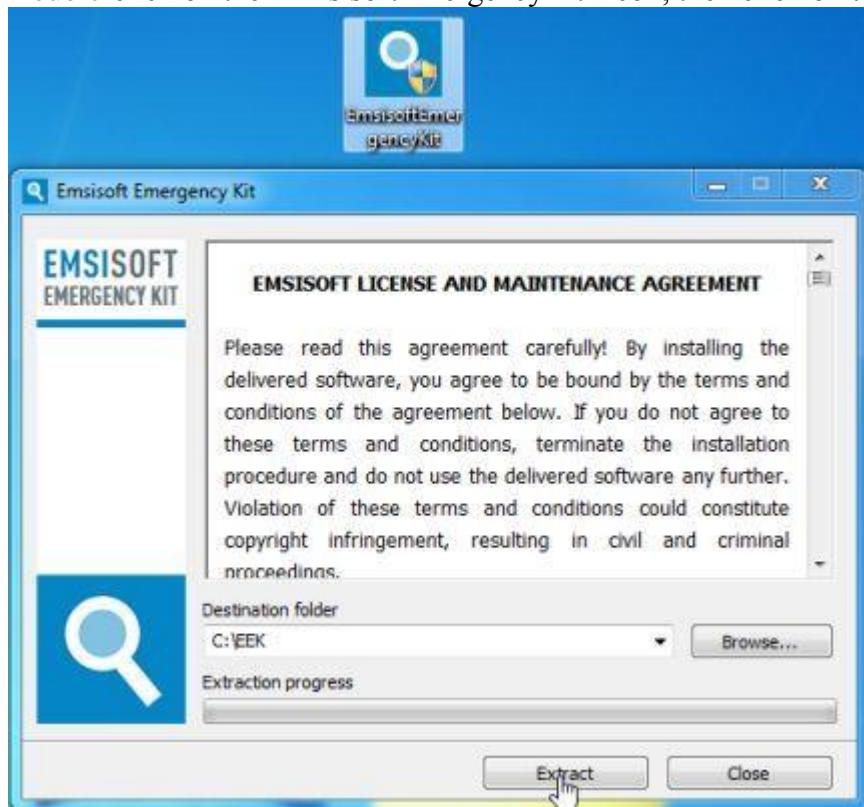


STEP 6: Double-check for any left over infections on your computer with Emsisoft Anti-Malware

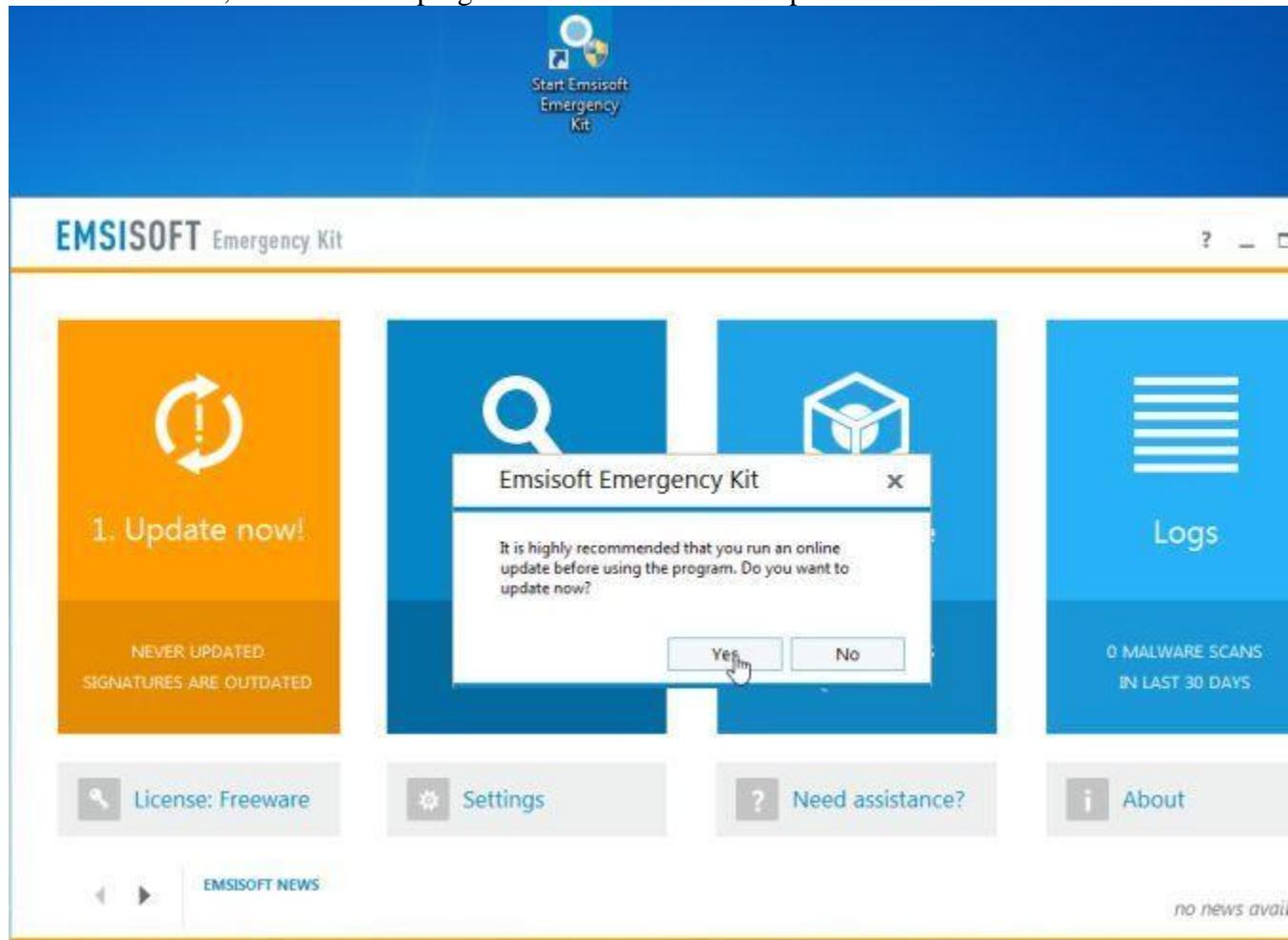
The Emsisoft Emergency Kit Scanner includes the powerful Emsisoft Scanner complete with graphical user interface. Scan the infected PC for Viruses, Trojans, Spyware, Adware, Worms, Dialers, Keyloggers and other malicious programs.

1. You can **download Emsisoft Emergency Kit** from the below link.
EMSIOSOFT EMERGENCY KIT DOWNLOAD LINK ((*This link will open a new web page from where you can download Emsisoft Emergency Kit*)

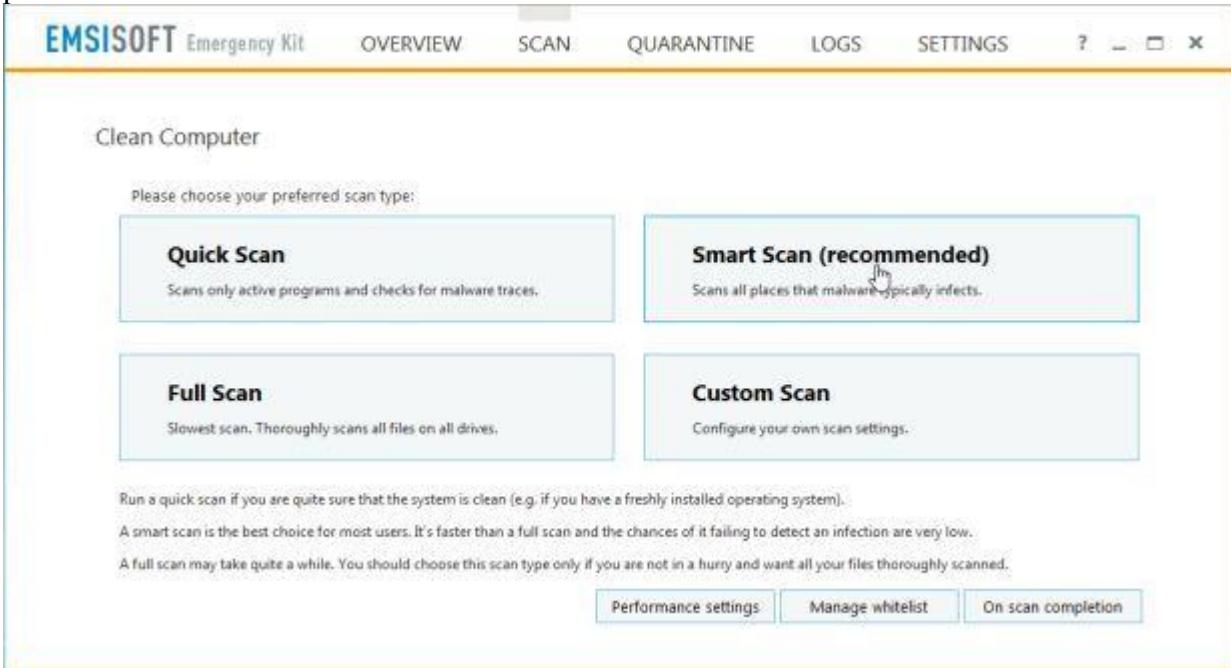
2. Double-click on the “EmsisoftEmergencyKit” icon, then click on the “Extract” button.



3. On your desktop you should now have a “Start Extract Emsisoft Emergency Kit” icon, double-click on it, then when the program will start allow it to update its database.



4. Once the Emsisoft Emergency Kit has update has completed, click on the “Scan” tab, and perform a “Smart Scan”.



5. When the scan will be completed, you will be presented with a screen reporting which malicious files has Emsisoft detected on your computer, and you'll need to click on Quarantine selected objects to remove them.

